TUNKEUTUMISTESTAUS

Mikko Järvinen

Opinnäytetyö
Joulukuu 2013
Tietojenkäsittely

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely

JÄRVINEN, MIKKO:
Tunkeutumistestaus

Opinnäytetyö 68 sivua, joista liitteitä 2 sivua
Joulukuu 2013

Työn tarkoituksena oli tuoda esille tunkeutumistestaukseen liittyvää teoriaa ja käytänteitä, jotta lukijalle muodostuu käsitys tunkeutumistestauksesta. Teoria osuus kostuu tunkeutumistestauksen määritelmistä sekä testaajan ammattitaidon kuvauksen. Tunkeutumistestaus käydään läpi painottaen Windows-järjestelmiä. Teoriaa on sovellettu käytäntöön todelliseen verkkoon tehdyllä haavoittuvuustestauksella.

Käytännön osuuden testaus osoitti, että järjestelmästä kuin järjestelmästä on mahdollisuus saada tietoja sovelluksilla, joista suurin oli ilmaisia, helposti saatavilla olevia. Moni sovellus oli käytettävissä englanninkielisenä. Kohdejärjestelmästä saatiin kerättyä DNS-tietoja, joiden pohjalta suoritettu porttiskannaus paljasti palveluita ja niiden versioita. Testauksen puitteissa suoritettiin myös käyttöjärjestelmän tunnistusta, jonka aikana tunnistettiin useita käyttöjärjestelmiä, joista jotkin sijaitsivat verkon laitteilla. Testauksen osana testattiin kohde verkon kestävyyttä erilaisten hyökkäysten aikana. Käytetyt hyökkäykset katkaisivat verkon toiminnan.

Tunkeutumistestaus on oleellinen osa tietoturvaa, mutta vain oikein käytettynä. Se on vähiten tunnettu tietoturvallisuuden alue, joka johtuu yhtäläisyyksistä hakkerointiin. Hakkerointi puolestaan yhdistetään rikolliseen toimintaan. Tunkeutumistestaus on kuitenkin tehokas osa tietoturvallisuutta, jos siitä vastaavat oikeat ihmiset, joilla on oikea koulutus.

Asiasanat: tunkeutumistestaus, tietoturva, hakkerointi

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems

JÄRVINEN, MIKKO:
Penetration Testing

Bachelor's thesis 68 pages, appendices 2 pages
December 2013

The purpose of this thesis was to bring out theory and practices concerning penetration testing. This provides the reader an understanding of the penetration testing process. The theory part consists of a discussion of what penetration testing means and what is required of an penetration tester, and a description of how penetration testing is implemented with emphasis on Windows systems. Theory part of the thesis was put into practice by means of doing a vulnerability analysis of a real network.

The practical part of the thesis proved that you can get information out of almost any network with applications that are a free and easily available. Most applications can be used if the user has some knowledge of the English language. The practical part consisted of information gathering by means of DNS information, port scanning, service identification, version identification and operating system identification. Information gathering revealed several crucial pieces of information on which further testing could be based on. Testing also included attacking the target to see how it holds up under attack. It was found that the services of the target system almost immediately.

Penetration testing is an integral part of information security but only if it is used properly. It is one of the lesser known areas of information security. Much of this is due to its resemblance to hacking. This in turn is associated with criminal activities. Penetration testing however is an effective part of information security if the right people with the right kind of training are in charge of it.

Key words: penetration testing, hackers, hacking, information security

SISÄLLYS

LYHENTEET JA TERMIT

ACL Access Control List. Reitittimillä käytettävä lista, joka sallii tai estää pääsyn verkkoon.

AD Active Directory. Microsoftin hakemistopalvelu Windows toimialueita varten.

ARIN American Registry for Internet Numbers. Yksi viidestä ICANN:n alaisesta RIR:stä. Vastaa Pohjois-Amerikan alueen ja joistakin Karibian sekä Pohjois-Atlannin saarien IP-osoitteista.

ARP Address Resolution Protocol. Protokolla, joka selvittää MAC-osoitteen IP-osoitteen perusteella.

DC Domain Controller. AD:ssa toimiva palvelin, joka vastaa esim. kirjautumisiin.

DF Don’t Fragment. IPv4-paketttiin liittyvä lippu, joka estää paketiin pilkkomisen matkan varrella.

DHCP Dynamic Host Configuration Protocol. Protokolla, jonka avulla IPv4 ympäristössä annetaan tietokoneille ja muille laitteille automaattisesti IP-osoitetiedot.

DNS Domain Name System. Järjestelmä, joka vastaa WWW-osoitteiden kääntämisestä IP-osoitteiksi.

DOS Denial Of Service. Verkkohyökkäys, jossa eri keinoin tehdään kohteen tarjoama palvelu käyttökelvottomaksi.

ICANN Internet Corporation for Assigned Names and Numbers. Internetin toiminnasta vastaava katto-organisaatio.

ICMP Internet Contol Message Protocol. Protokolla, jota laitteet käyttävät esim. virheilmoitusten välittämiseen. Myös esim. ping käyttää ICMP:tä liikenteensä kuljettamiseen.

IDS Intrusion Detection System. Laite tai sovellus, joka tarkkailee verkkoa tavallisuudesta poikkeavan liikenteen varalta.

IKE Internet Key Exchange. IPsec:n käyttämä protokolla tietoturvallisten yhteyksien muodostamiseen.

IPS Intrusion Prevention System. Laite, joka tarkkailee verkkoa ja yrittää estää sinne kuulumatonta liikennettä.

IPSec Internet Protocol Security. Protokollaperhe, jonka avulla voidaan salata ja todentaa tavanomaista IP liikennettä.

LDAP Lightweight Directory Access Protocol. Hakemistojen yhteysprotokolla.

LM LAN Manager. Microsoftin ja 3Com:n yhteistyössä kehittämä verkkokäyttöjärjestelmä, jonka salasanojen todennus on haavoittuvainen.

LPT Licensed Penetration Tester. EC-Council:n myöntämä tietoturva-alan sertifikaatti.

LSA Local Security Authority. Windows käyttöjärjestelmän osa, joka vastaa kirjautuvien käyttäjien todentamisesta, salasanojen muutoksista ja pääsy valtuuksien luomisesta..

NTLM NT LAN Manager. Kokoelma Microsoftin tietoturvaprotokollia, jotka tarjoavat todennuksen, koskemattomuuden ja luottamuksellisuuden.

RDC Remote Desktop Connection. Microsoftin Remote Desktop Services asiakassovellus.

RID Relative IDentifier. Microsoftin AD:hen liittyvä vaihtuvan pituinen numerosarja, joka annetaan objektille sen luonnin yhteydessä ja sitä käytetään osana SID:ä.

RIPE Réseaux IP Européens. Yksi viidestä ICANN:n alaisesta RIR:stä. RIPE vastaa Euroopan, Venäjän, Lähi-Idän ja Keski-Aasian IP-osoitteista.

RIR Regional Internet Registries. Organisaatio, joka vastaa omalla alueellaan IP-osoitteiden ja AS-numeroiden jakamisesta sekä rekisteröinnnistä.

RPC Microsoft Remote Procedure Call. Keino, joka mahdollistaa sovelluksen käynnistää prosesseja etänä, jotka kuitenkin näyttävät kuitenkin paikallisilta prosesseilta.

SAM Security Accounts Manager. Tiedosto, joka sisältää Windows käyttäjien salasanojen tarkisteet.

SID Security Identifier. Windows käyttöjärjestelmän käyttäjille, käyttäjäryhmille tai muille todennettaville osille annettava tunniste, joka koostuus mm. RID:stä.

SMB Server Message Block. Sovellustason protokolla, jota käytetään mm. tiedostojen ja tulostimien jakamiseen verkossa.

SOA Start Of Authority. DNS tietue, joka kertoo esimerkiksi ensijaisen DNS-palvelimen.

TFTP Trivial File Transfer Protocol. Tiedostojen siirtoprotokolla, jota käytetään usein asetus- tai käynnistystiedostojen siirtämiseen automaattisesti.

TS Terminal Services. Nykyään Remote Desktop Service. Mahdollistaa sovellusten ja tietojen käytön etäyhteyden yli.

TTL Time To Live. Arvo, joka kertoo kuinka kauan paketti voi kiertää verkossa.

VNC Virtual Network Computing. Tietokoneiden etähallintakeino.

VPN Virtual Private Network. Keino, jolla luodaan yksityinen verkko julkisen verkon rinnalle.

1 JOHDANTO

Tietoturvallisuutta miettiessä tulee varmasti mieleen tietoturvapolitiikka, palomuurit, virustutkat ja muita melko perinteisiä tietoturvallisuuteen liitettäviä elementtejä. Nämä ovatkin tietoturvallisuuden olennaisia osia, joita ilman ei tietoturvallista ympäristöä voisi muodostaa. Tehtyjen tietoturvaratkaisujen toimivuudesta voidaan kuitenkin esittää vain hataria arvioita, sillä ala kehittyy jatkuvasti. Siksi tietoturvaratkaisut tulisi testata perusteellisesti. Tällöin puhutaan tunkeutumistestauksesta.

Tämän työn tavoitteena on esitellä tunkeutumistestausta. Tavoite saavutetaan esittelemällä tunkeutumistestauksen käytänteitä ja teoriaa, jotta aiheesta voisi muodostaa kattavan käsityksen. Teoriaa sovelletaan käytäntöön suorittamalla haavoittuvuustestaus oikeaan verkkoon.

Työn tuloksia voivat hyödyntää kaikenkokoiset organisaatiot tietoturvallisuuden tilaan katsomatta, sillä mikään järjestelmä ei ole täydellinen. Tuloksien avulla voisi esittää oikeita kysymyksiä, jos tietoturvatyö on ulkoistettu, ja toiminnassa olevien järjestelmien toimintaa voidaan tarkastaa ja syventää.

Työssä ei käsitellä tietoturvapolitiikan muodostamista, palomuurien, virustutkien yms. sovellusten asentamista, vaikkakin niiden käyttöä kommentoidaan, sikäli kun se on tarpeellista asian esittämisen kannalta. Perusasioita, kuten esimerkiksi IP-osoitteiden toimintaa, käsitellään vain, sillä tasolla minkä varsinaisen aiheen esittäminen vaatii.

Tunkeutumistestaus voi eri yhteyksissä käsittää monia eri asioita, kuten esimerkiksi erilaisten langattomien teknologioiden tai fyysisten suojakeinojen testausta. (Federal Office for Information Security 2003, 7; NIST 2008, 4-6 — 4-10.) Tässä työssä keskitytään tunkeutumistestaukseen siltä osin, kun se koskee lähiverkon testaamista.

2 TUNKEUTUMISTESTAUKSEN PERUSTEET

Tunkeutumistestauksella tarkoitetaan kohdeorganisaation verkon järjestelmällistä testaamista tietoturva-aukkojen paljastamiseksi. Testaamisen aikana simuloidaan erilaisia hyökkäyksiä kohdeverkkoon. Karkealla tasolla testaamisen ja hakkeroinnin ero on siinä, mitä tiedolla tehdään ja onko asiasta sovittu asianmukaisesti etukäteen. (Klevinsky, Laliberte & Gupta 2002, 9,19.)

2.1 Tunkeutumistestaustyypit

Tunkeutumistestaus voi olla **ennalta ilmoitettua** tai **ilmoittamatonta**. Se kumpaa tyyppiä käytetään, riippuu siitä, mitä halutaan testata. Ennalta ilmoitetussa testissä kohteena on itse järjestelmä, ja siinä työskennellään asiakkaan tietoturvasta vastaavien kanssa yhteistyössä, usein keskittyen kohdeverkon tärkeimpiin osiin. Tämän kaltaisen testin etuna on myös se että organisaation tietoturvasta vastaavilla ihmisillä on mahdollisuus samalla oppia. (Klevinsky ym. 2002, 25 — 27; Kennedy, O'Gorman, Kearns & Aharoni 2011, 5.)

Ilmoittamattomassa testauksessa sen parametreista ja ajankohdasta eivät tiedä muut kuin yrityksen ylimmät tahot. Tämän kaltaisessa testauksessa tarkoitus onkin testata yrityksen tietoturvasta vastaavan henkilökunnan toimintaa tilanteessa, jossa järjestelmää vastaan hyökätään, sekä voimassa olevien tietoturvaratkaisujen kestävyyttä. Toisin kuin ennalta ilmoitetussa testauksessa ilmoittamattomassa joudutaan testaukseen vaadittavat tiedot keräämään itse järjestelmästä ja muista tietolähteistä. Tästä johtuen tämä testaustyyppi vaatii testaajalta enemmän taitoja. Ilmoittamaton testi on lähempänä todellista tilannetta, ja sitä käytetäänkin enemmän tästä syystä. Usein tämän testauksen tulokset ovat paljon käyttökelpoisempia kuin ilmoitetun testauksen, sillä laitteiden ja sovellusten lisäksi testataan tietoturvaratkaisujen toimivuus. (Klevinsky ym. 2002, 25 — 27; Kennedy ym. 2011, 5.)

2.2 Testauksen määrittely

Testauksen aikana testaaja pääsee käsiksi asiakkaan tietoihin, jotka ovat usein arkaluontoisia. Testauksen määrittelyn ja varsinaisen testauksen aikana testaajalle kertyy myös

tietoja järjestelmän heikkouksista. Asiakas haluaa näiden tietojen pysyvän salassa ja tästä syystä allekirjoitetaan salassapitosopimus osana testaussopimusta. (PTES 2012; Wai 2002, 4; Orrey, K. 2013.)

Testauksen määrittelyn tarkoituksena on antaa testaukselle *rajat*, jotka määrittelevät mitä testataan sekä *miten testataan*. Aika on tärkeä osa testausta ja rajojen puitteissa sillä tarkoitetaan aikaväliä, jolla testaus suoritetaan. Kohdeverkosta on hyvä sopia myös ne IP-osoitteet (Internet Protocol), jotka ovat testauksessa mukana, vaikka kyse olisi pienestä verkosta. Sama koskee myös asiakkaan toimialueita ja verkkotunnuksia. Varsinkin suurten asiakasorganisaatioiden tapauksessa tulee ottaa huomioon, miten organisaatioiden palvelut on toteutettu. Esimerkiksi jos asiakkaan tietoja on tallennettu pilvipalveluun, jossa samalla fyysisellä medialla sijaitsee muidenkin organisaatioiden tietoja. Asiakkaan internetyhteydentarjoaja voi normaalisti rajoittaa testaukseen liittyvää verkkoliikennettä, mutta saattaa tarjota mahdollisuuksia testaamista varten. Riippuen testauksen tyypistä voi olla tarpeellista määritellä, mitä osia tietoturvapalveluista testataan. Tämä on erityisen tärkeää silloin, kun tietoturvapalveluista vastaa kolmas osapuoli. Moni asia testauksessa liittyy lakiasioihin, ja testauksen rajoja määritellessä tämä tulee ilmi, jos testauksen rajaamia laitteita sijaitsee toisissa maissa tai internetyhteydentarjoajan tiloissa. Tällöin on hyvä varmistua laitteen sijaintimaan tunkeutumistestausta koskevasta lainsäädännöstä. (PTES 2012; Wai 2002, 4.)

Testauksen rajoja asetettaessa määritellään, milloin testaus alkaa ja loppuu. On myös määriteltävä alun ja lopun välinen osa eli se, mitä testausta suoritetaan missäkin vaiheessa. Osana tätä määrittelyä otetaan kantaa myös sijaintiin. Matkustaako testaaja asiakkaan tiloihin vai hyödynnetäänkö esimerkiksi VPN-yhteyttä (Virtual Private Network). Säännölliset tapaamiset testauksen edistymisestä pitävät asiakkaan ajan tasalla. Ajan ollessa merkittävä osa testauksen määrittelyä ja asiakkaan päivittäisen toiminnan jatkuessa testauksen ajan, on hyvä määritellä ne aikavälit päivästä, jolloin testausta saa suorittaa. (PTES 2012; Wai 2002, 4.)

Kaikki projektit tarvitsevat aikarajan ja rajat joissa toimia, mutta mikään projekti ei toimi ilman tavoitteita. Tunkeutumistestauksen tavoitteet liittyvät oleellisesti asiakkaan liiketoimintaan, ei erilaisten auditointien läpäisyyn, vaikka ne voisivatkin olla syy testaukselle. Tavoitteiden määrittely on hyvä aloittaa tutkimalla, mikä on asiakkaan tietoturvallisuuden taso. Näin voi tarjota asiakkaalle parempaa ja tarkempaa palvelua, sillä asi-

akkaalla ei välttämättä ole mitään käsitystä tunkeutumistestauksesta. Näin ollen asiakas saa arvokkaampaa tietoa, jos ensiksi suoritetaan vain haavoittuvuusanalyysi. (PTES 2012; Wai 2002, 4.)

Määrittelyn tukena käytetään usein myös kyselyitä, joiden avulla määritellään monia testauksen tärkeitä yksityiskohtia, kuten esim. ajankohdat, mitkä keinot ovat sallittuja testauksessa sekä yleisesti testauksen syvyyttä. Joidenkin kohdeverkkojen laitteistoon saattaa kuulua fyysisiä tai softapalomuureja, IPS- tai IDS-järjestelmiä tai kuormantasauslaitteita. Kaikki nämä laitteet voivat vaikuttaa testauksen suorittamiseen ja tuloksiin ja niistä on hyvä olla perillä jo testausta aloittaessa. On myös hyvin oleellista selvittää mitä saa ja mitä ei saa tehdä koneella, jonka kautta verkkoon on päästy. (PTES 2012; Federal Office for Information Security 2003, 16; The SANS Insitute 2010.)

Riippuen siitä millaista testausta tehdään, voidaan kyselyt laajentaa käsittämään myös järjestelmän ylläpitäjät, joilla monesti on kriittistä tietoa järjestelmän kunnosta ja haavoittuvuuksista. He tietävät, onko kohdeverkon järjestelmissä käytössä vanhoja sovelluksia tai käyttöjärjestelmiä, onko kohdeverkossa sellaisia osia, jotka eivät ole organisaation hallinnassa, käytetäänkö sovelluksia, jotka tarkkailevat verkon toimintaa ja mitkä ovat kohdeverkon kriittisimmät sovellukset ja palvelimet. (PTES 2012; Stanford University 2007.)

Jos testauksessa suoritetaan DOS-hyökkäys, on tärkeää suorittaa kysely myös liiketoimintayksiköiden johtajille. Nämä johtajat tietävät tai ainakin heidän tulisi tietää, minkä tiedon julkiseksi tuleminen tai jonkinasteinen tuhoutuminen olisi katastrofaalista organisaatiolle, ja he tuntevat myös ne menetelmät, joiden avulla ongelmatilanteista palaudutaan. (PTES 2012.)

2.3 Sisäinen ja ulkoinen tunkeutumistestaus

Tunkeutumistestaus voidaan jakaa jo mainittujen tapojen lisäksi myös *ulkoiseen* ja *sisäiseen* testaukseen. Nämä kaksi tyyppiä voidaan molemmat suorittaa ennalta ilmoitettuna tai ilmoittamattomana.

2.3.1 Ulkoinen tunkeutumistestaus

Ulkoisen tunkeutumistestauksen tarkoituksena on tunnistaa ne haavoittuvuudet, jotka altistavat asiakkaan verkon tai yhteydet verkon ulkopuolelle, hyökkäyksille. (SANS Institute 2002, 4.) Suurin osa tunkeutumistestauksen keinoista on käytettävissä sekä ulkoisessa että sisäisessä testauksessa, mutta esimerkiksi julkisten tietolähteiden hyödyntäminen on hyödyllisimmillään ulkoisessa testauksessa.

2.3.2 Sisäinen tunkeutumistaus

Sisäisessä testauksessa testaaja voi sijaita organisaation tiloissa tai testaus voidaan suorittaa etänä. Sisäisen testauksen määrittelyssä on otettava huomioon että monet verkon turvallisuudesta vastaavat laitteet, kuten palomuurit ja IDS:t (Intrusion Detection System), on jo ohitettu. (Klevinsky ym. 2002, 91 — 92.)

Sisäisessä testauksessa testauksen alkuasetelma on erilainen ja se vaihtelee tapauksittain. Tällaisia alkuasetelmia voisi esimerkiksi olla paha konsultti, vihainen työntekijä ja epärehellinen siivooja. Pahan konsultin asetelmassa asiakkaalta pyydetään samanlaiset oikeudet kuin konsultille annettaisiin vastaavassa tilanteessa. Vihaisen työntekijän asetelmassa käytetään normaaleja työntekijöille annettavia käyttäjätunnuksia. Epärehellisen siivoojan asetelmassa käytetään niitä tunnuksia, jotka onnistutaan selvittämään. Käyttäjätunnusten lisäksi testaaja tarvitsee asianmukaiset henkilökortit sekä kulkuluvat. Organisaation piiristä on sovittava yhteyshenkilö, jonka kanssa testausta voi koordinoida, tämä auttaa myös suojaamaan testaajaa perättömiltä syytöksiltä. (Klevinsky ym. 2002, 92.)

Pahan konsultin alkuasetelmassa testaaja asettuu asiakkaan tiloihin, johonkin erilliseen työtilaan. Laitteistona toimii testaajan oma kannettava tietokone tai asiakkaan, riippuen asiakkaan tietoturvapolitiikasta ja testauksen määrittelystä. Vihaisen työntekijän asetelmassa lähdetään nimen mukaisesti sellaisesta tilanteesta, jossa yrityksen työntekijäkin olisi. Epärehellisen siivoojan alkuasetelmassa käytetään laitteistona omaa kannettavaa tai hyödynnetään asiakkaan työasemia työajan ulkopuolella. (Klevinsky ym. 2002, 92–93.)

2.4 Mitä vaaditaan testauksen suorittajalta

Testaajan pitää tuntea paljon erilaisia teknologioita: käyttöjärjestelmät, reitittimet, kytkimet, palomuurit, IDS, IPS, pakettianalysaattorit, auditointityökalut ja autentikointimekanismeja. Vaikka haluaisi olla asiantuntija kaikissa teknologioissa, on hyvä kuitenkin tunnustaa omat rajansa ja olla asiantuntija muutamassa. Testaajalle on hyötyä jo pelkän toimintaperiaatteen ymmärtämisestä, sillä pääsee usein jo etsimään keinoa kyseisen teknologian kiertämiseen. Teknisen tietämyksen lisäksi testaajalle on huomattavaa arvoa myös dokumentointi- ja projektinhallintaidoista. (Klevinsky ym. 2002, 22 — 25; International Journal of Advanced Science and Technology 2009, 3 — 4; 0x0e.org | pentesting perspective 2008.)

Työkaluihin pätee sama periaate kuin teknologioihin, niitä on paljon ja ei ole järkevää yrittää tuntea kaikkia läpikotaisin. ”Työkalupakki” tuskin pysyy samana testitapauksesta toiseen, vaan sitä muokataan kunkin tapauksen mukaan ja uusia työkaluja löydettäessä. Ihanteellisessa tilanteessa testaaja tuntee, jonkin työkalun, jokaiseen testauksen vaiheeseen. Riippuen siitä millaista testausta tekee, asettaa se erilaisia vaatimuksia laitteistolle. Ihanteellinen valinta testaajalle on kannettava tietokone, sillä se soveltuu erinomaisesti sisäiseen tunkeutumistestaukseen, mutta pöytäkone soveltuu myös testaamiseen ja saattaa olla parempi ratkaisu joissakin tilanteissa. (Klevinsky ym. 2002, 23, 158 — 159; International Journal of Advanced Science and Technology 2009, 4 — 8.)

Tärkeää tunkeutumistestauksen alalla työskenteleville on luottamus. Asiakkaiden on voitava luottaa siihen että testaaja toimii eettisesti joka hetki tutkiessaan kohde järjestelmää. On testaajan tehtävä huolehtia omasta luotettavuudestaan, jota on vaikea saada takaisin sen kerran menetettyään. (Klevinsky ym. 2002, 24 — 25; Schreiber, S. 2009.)

2.5 Ammattitaito

IT-alalla, niin kuin monella muullakin alalla, osaamista osoitetaan erilaisilla tutkinnoilla tai sertifikaateilla. Tässä mielessä tunkeutumistestaus ei ole mikään poikkeus. Tunkeutumistestausalalla sertifikaatteja ja niihin liittyvää koulutusta hallinnoi mm. IACRB. Sertifikaatteja on eritasoisia ja jossakin niissä keskitytään esimerkiksi sovellusten tunkeutumistestaukseen. Perustason sertifikaatti on CPT (Certified Penetration Testing), josta jatketaan CEPT (Certified Expert Penetration Tester) sertifikaattiin. IACRB:n

lisäksi sertifikaatteja myöntää esimerkiksi International Council of E-Commerce (EC-Council) consultants, jonka sertifikaatit CEH (Certified Ethical Hacker) ja LPT (Licensed Penetration Tester) soveltuvat tunkeutumistestauksen alalle. Näiden kahden lisäksi SANS myöntää tunkeutumistestausalan sertifikaatteja GIAC (Global Information Assurance Certification) ohjelmansa kautta. (IACRB 2009; EC-Council 2013; SANS 2013; GIAC 2013.)

Edellä mainitut tahot eivät ole ainoat tahot, jotka myöntävät tunkeutumistestaus alan sertifikaatteja. Suomesta löytyy ainakin Mile2:sen myöntämien sertifikaattien CPTE (Certified Penetration Testing Engineer) ja sen jatko sertifikaatin CPTC (Certified Penetration Testing Consultant) koulutusta jota järjestää KPMG. Se järjestää myös koulutusta CPEH (Certified Professional Ethical Hacker) sertifikaattiin liittyen. CPTE-koulutuksessa opitaan etsimään haavoittuvuuksia ja murtautumaan Ethernet- ja WLAN-verkkoihin (Wireless Local Area Network), käyttöjärjestelmiin, sovelluksiin ja web-ympäristöihin. Sertifikaatin jatkokoulutuksessa keskitytään syventämään aikaisemman koulutuksen aikana opittua. (mile2 2013; KPMG 2013.)

3 TUNKEUTUMISTESTAUKSEN VAIHEET

Tunkeutumistestaus voidaan jakaa neljään päävaiheeseen:

1. Suunnittelu – Määritellään testaus ja huolehditaan asianmukaisista sopimuksista.
2. Tutkimus – Kerätään tietoja verkosta. Koostuu kolmesta osasta:
    a. Järjestelmän jalanjälkien tutkiminen
    b. Skannaus
    c. Haavoittuvuuksien analysointi
3. Hyökkäys.
    a. Todentamattomat hyökkäykset
    b. Todennetut hyökkäykset
    c. Oikeuksien lisääminen
4. Raportointi

(Saindane 2013, 4.)

3.1 Suunnittelu

Suunnitteluvaiheessa määritellään testauksen parametrit (kts.kpl 2.2) ja huolehditaan että asianmukaiset sopimukset on allekirjoitettu ennen testauksen aloittamista. Tarkan määrittelyn avulla testaaja voi alustavasti valita testaukseen käytettäviä ohjelmistoja.

3.2 Tutkimus

Ennen kuin suoritetaan mitään varsinaisia hyökkäystoimintoja, olisi suotavaa tuntea kohde mahdollisimman hyvin. Kohteesta halutaan tietää ne laitteet, jotka ovat todellisia kohteita, kohteen verkon rakenne sekä millaista liikennettä verkko sallii. Hankittujen tietojen perusteella voi löytää kohteeseen sopivia hyökkäyskeinoja. (Klevinsky ym. 2002, 52.)

3.2.1 Järjestelmän jalanjäljet

Tutkimus alkaa keräämällä taustatietoja kohteesta, joille testauksen myöhemmät vaiheet perustuvat. Taustatietojen kerääminen on järjestelmällistä toimintaa, jonka lopputulok-

sena testaajalle muodostuu kuva kohteesta. Usein tiedon etsintä alkaa julkisesti saatavista tiedoista. Näihin tietoja voidaan hankkia yrityksen verkkosivuilta, sijaintitiedoista, työntekijöistä, ajankohtaisista tapahtumista, arkistoiduista tiedoista sekä hakukoneista ja niihin liittyvistä tiedoista. (McClure ym.. 2012, 8 — 11.)

Yrityksen verkkosivuilta saa tietoja lukemalla niitä, mutta arvokkaita tietoja on voitu piilottaa myös verkkosivujen HTML-koodin joukkoon kommenttien muodossa. Tiedon etsintä HTML-koodin joukosta on huomattavasti tehokkaampaa, jos koko sivun lataa itselleen, näin materiaalin läpi käynnin voi suorittaa ohjelmallisesti. Yritykset saattavat käyttää tunnetun www-osoitteen lisäksi muitakin osoitteita, kuten esimerkiksi http- ja https-alkuisia sekä http://www1 yms. muunnoksia. Näitä www-osoitteita ei tule unohtaa tiedonkeruun yhteydessä. Yrityksen resursseihin saattaa olla pääsy Internetin kautta. Tämän kaltaisesta palvelusta toimii hyvin esimerkkinä Microsoftin Outlook, joka siis usein löytyy jollakin ilmiselvällä nimellä Internetin kautta esim. https:owa.esimerkki.com tai https:outlook.esimerkki.com. Toinen esimerkki liian paljastavasta nimestä on esimerkiksi https://vpn.esimerkki.fi. Nämä palvelut, riippuen konfiguraation tasosta, saattavat antaa paljonkin oleellista tietoa itsestään, ja niiden olemassaolo on jo itsessään tärkeä tieto. (McClure ym.. 2012, 12; Sutton, E. 2013, 7; Know The Trade 2013.)

Yritysten yhteistyökumppanit ovat myös otollinen tietolähde, sillä yhteistyökumppaneille saatetaan usein tarjota käyttöön loppupään yhteyksiä omiin palveluihin. Näitä yhteistyökumppaneita voidaan hyödyntää suorasti tai epäsuorasti testauksen hyökkäysvaiheessa. (McClure ym.. 2012, 13.)

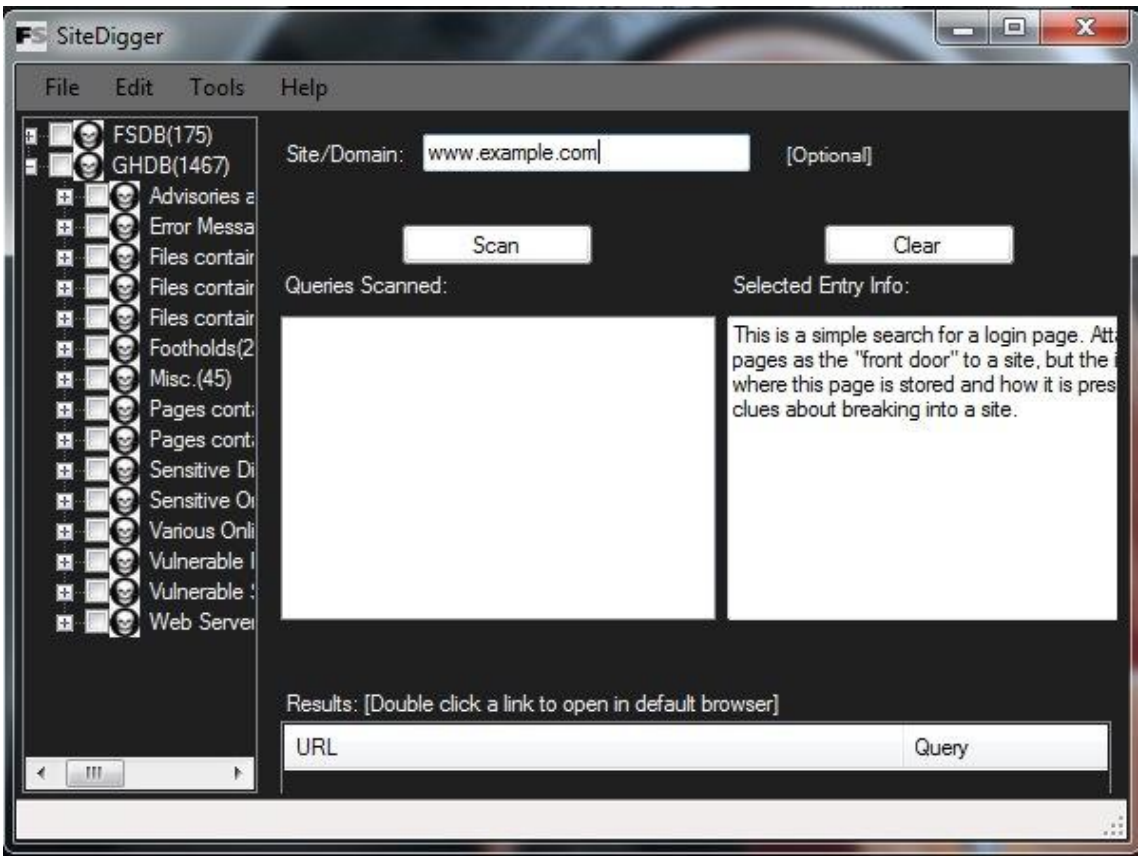
Valtaosa tunkeutumistestauksesta perustuu jonkin laitteen tai sovelluksen käyttöön, mutta tiedonkeräämiseen liittyy keinoja, joissa ei hyödynnetä kumpaakaan. Pelkästään yrityksen fyysinen sijainti saattaa olla todella arvokas tieto, sillä sen avulla voi olla mahdollista päästä käsiksi yrityksen roskiin heittämiin papereihin tai muuhun materiaaliin, joista puolestaan voi selvitä teknisiä tietoja tai muita tietoja, joita voi hyödyntää sosiaalisessa manipuloinnissa. Fyysisen sijainnin perusteella voisi suorittaa myös tarkkailua sekä fyysistä tunkeutumista. Näissä keinoissa on otettava huomioon testauksesta tehty sopimus. (McClure ym.. 2012, 14 — 15; Penetration Testing Lab 2013.)

Sosiaalisia tiedonkeruukeinoja hyödyntävät löytävät käyttökelpoisia tietoja yritysten työntekijöistä. Yritysten verkkosivut ovat hyvä lähtökohta tiedonhankinnalle sen työntekijöistä, mutta niiden tarjoamilla tiedoilla ei välttämättä pääse kovinkaan pitkälle. Erilaiset sosiaalisen median sivustot (esim. facebook ja linkedin) kelpaavat erinomaisesti tietolähteiksi työntekijöistä. Yrityksen työilmoitukset saattavat paljastaa yrityksen käyttämiä laitteita ja sovelluksia. Yrityksestä voi saada oleellista tietoa seuraamalla siihen liittyviä ajankohtaisia uutisia, joista voi esimerkiksi paljastua että jokin palvelu on ulkoistettu tai yhteistyön aloittaminen uuden yhteistyökumppanin kanssa. Entisten työntekijöiden ylläpitämät sivut yrityksestä, jotka eivät välttämättä käsittele yritystä hyvässä valossa, kannattaa hyödyntää tietolähteenä. (McClure ym. 2012, 16 — 19; Know The Trade 2013.)

Yrityksen sivuilla on joskus menneisyydessä saattanut olla testaajan (tai hyökkääjän) kannalta tärkeitä tietoja, mutta ne on sittemmin poistettu, joka ei tarkoita että ne olisi menetetty. Testaajan käyttöön löytyy esimeriksi WayBack Machine palvelu (archive.org), josta voi etsiä arkistoituja www-sivuja. Myös Googlen välimuistiin tallentuneita www-sivuja voi saada käyttöönsä (”cache:” www-sivun osoitteen eteen). (McClure ym.. 2012, 19 — 20; Web Applications Stack Exchange. 2012.)

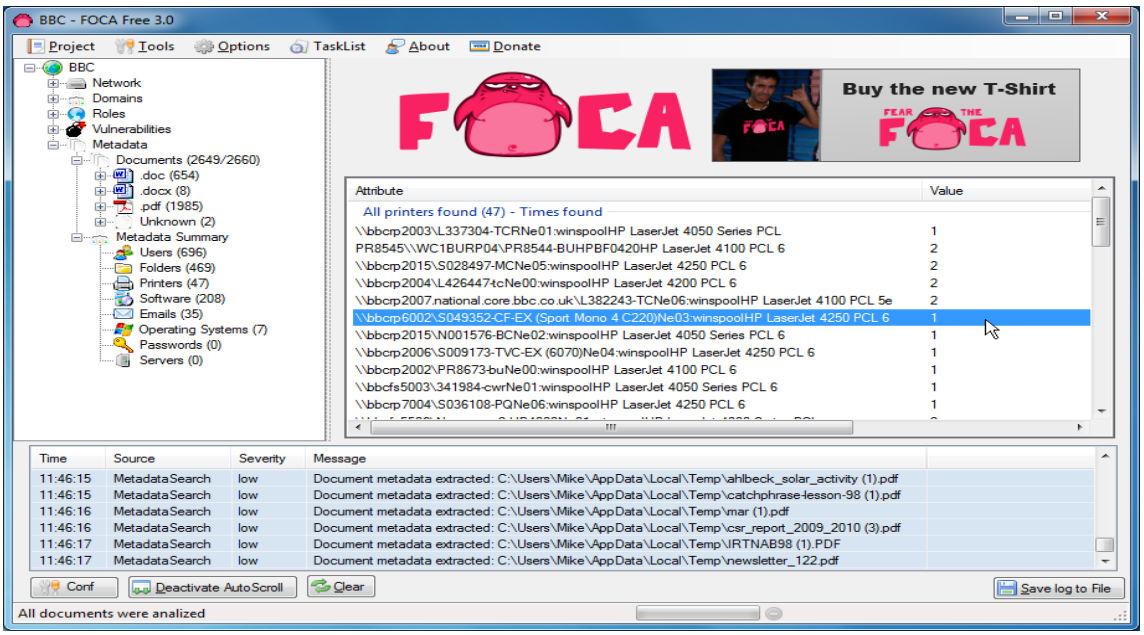
Hakukoneista, pääasiassa Googlesta, saa irti paljon muutakin tietoa kunhan sitä osaa etsiä. Googlen hakukoneeseen sisältyy useita komentoja, joiden avulla saa etsittyä tietoja tunkeutumistestauksen käyttöön. Esimerkiksi syöttämällä komento ”intitle:"Remote Desktop Web Connection" inurl:TSWeb/” Googlen hakuun saadaan tulokseksi sellaisia kohteita, joilla on käytössään Microsoftin RDC (Remote Desktop Connection) Web Connection. (McClure ym.. 2012, 20 — 21; Hackers For Charity 2013, 2004.)

Hakukoneiden hyödyntäminen tiedonhaussa yksittäisten hakujen avulla on todella aikaa vievää. Ajan säästämiseksi on olemassa useita sovelluksia testaajan käyttöön. Kuvasta 1 voidaan nähdä, kuinka SiteDigger -sovelluksella voi yhdistää useita Googlen hakukomentoja GHDB:stä (Google Hack DataBase). (McClure ym.. 2012, 22 — 24; Hackers For Charity 2013.)



Kuva 1: SiteDigger (Chandel, R. 2013)

FOCA, esitetty kuvassa 2, niminen sovellus voi etsiä www-sivuilta tiettyjä dokumentteja ja lisäksi tutkia niiden metadataa. FOCA:an on myös sisällytetty SHODAN hakutoiminto. Sen avulla voidaan etsiä Internetiin kytköksissä olevia järjestelmiä. (McClure ym.. 2012, 22 — 24.)



Kuva 2: FOCA (Williams, M. 2011)

Kun ryhtyy etsimään tietoja liittyen verkkotunnuksiin ja IP-osoitteisiin on hyvä muistaa että, vaikka molemmista vastaa sama katto-organisaatio (ICANN), ne rekisteröidään erikseen. Tästä johtuen ne löytyvät eri lähteistä. (McClure ym. 2012, 28 — 29; ICANN 2013.)

Monilla www-sivuilla tarjotaan WHOIS-haku mahdollisuutta, mutta on mahdollista että haku ei tuota lainkaan tuloksia. Siinä tapauksessa ratkaisu on tehdä haku osissa. Ensiksi pitää selvittää kuka vastaa kyseisistä verkkotunnuksista (esim. fi). Kuvasta 3. nähdään että fi verkkotunnuksista vastaa Ficora(www.ficora.fi.)

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:       FI

organisation: Finnish Communications Regulatory Authority
address:      PO Box 313
address:      Helsinki  FI-00181
address:      Finland

contact:      administrative
name:         Domain Names
organisation: Finnish Communications Regulatory Authority
address:      PO Box 313
address:      Helsinki  FI-00181
address:      Finland
phone:        +358 295 390 200
fax-no:       +358 295 390 270
e-mail:       firootadmin@ficora.fi
```

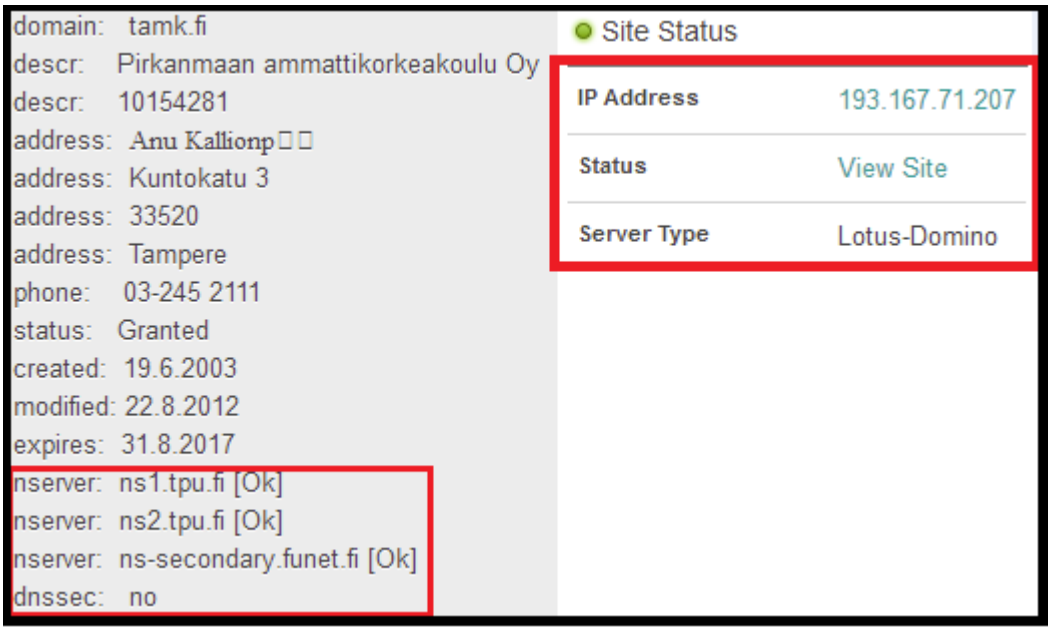
Kuva 3: fi verkkotunnuksien haku whois.iana.org:sta

Haun avulla selvisi kuka vastaa tietyistä verkkotunnuksista (merkittynä kuvaan 3). Ficoran sivuilla tehty haku tuotti suppeat tulokset, niiden olennaisin osa löytyy kuvassa 4. (McClure ym.. 2012, 29 — 31.)

Nimipalvelin	Tila
ns1.tpu.fi	Toimiva
ns2.tpu.fi	Toimiva
ns-secondary.funet.fi	Toimiva

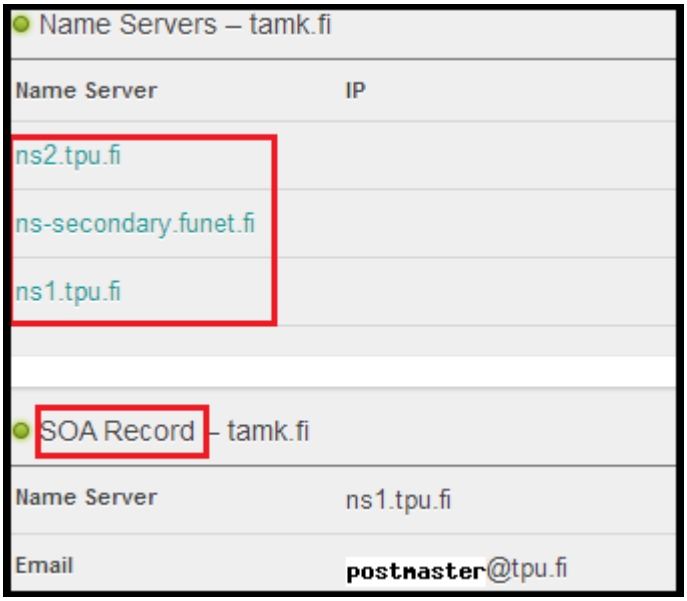
Kuva 4: Ficoran sivuilla tehty haku osoitteesta www.tamk.fi

Kuvissa 5-7 vastaava haku on suoritettu osoitteessa who.is, joka antoi huomattavasti kattavammat tulokset osoitteesta www.tamk.fi. Kuvan 5 esittämät tulokset vastaavat pääosin kuvan 4 tuloksia, mutta lisäksi siinä on kyseisen www-sivun IP-osoite.



Kuva 5: who.is osoitteessa suoritetun haun tuloksia

Kuvassa 6 on who.is osoitteesta tehdyn haun DNS:ää (Domain Name System) koskevia tuloksia. Nimipalvelimet ovat samat kuin kuvassa 4, mutta niiden lisäksi haussa on selvinnyt se nimipalvelin, jolla on SOA (Start Of Authority) tietue. (Microsoft 2013.)



Kuva 6: who.is osoitteessa tehdyn haun DNS-tulokset

Kuvassa 7 on lisää www.tamk.fi osoitteeseen liittyviä DNS tietoja. WWW-osoitteiden ja DNS tietueiden lisäksi tuloksista selviää IP-osoitteita sekä sähköposti-palvelimen olemassaolo.

DNS Records – TAMK.FI

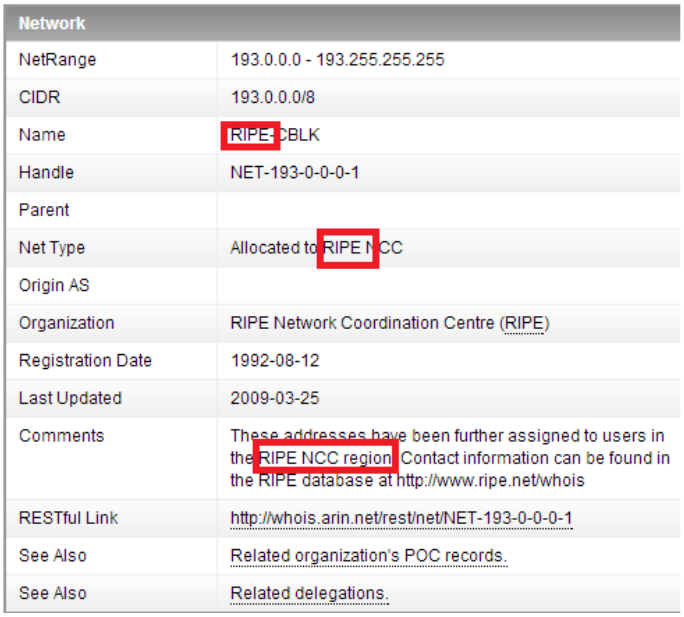
Record	Type	TTL	Priority	Content
tamk.fi	A	3 hours		193.167.71.207 (Tampere, 15, FI)
tamk.fi	MX	3 hours	10	smtp.tamk.fi
tamk.fi	NS	3 hours		ns2.tpu.fi
tamk.fi	NS	3 hours		ns-secondary.funet.fi
tamk.fi	NS	3 hours		ns1.tpu.fi
smtp.tamk.fi	A	3 hours		193.167.71.24 (Tampere, 15, FI)
tamk.fi	SOA	3 hours		ns1.tpu.fi. postmaster.tpu.fi. 2013070802 3600 900 604800 3600
tamk.fi	TXT	3 hours		Tampereen ammattikorkeakoulu
tamk.fi	TXT	3 hours		v=spf1 mx a:mta91.tamk.fi ~all
tamk.fi	SOA	1 hour		ns1.tpu.fi. postmaster.tpu.fi. 2013070802 3600 900 604800 3600
mail.tamk.fi	A	3 hours		193.167.71.59 (Tampere, 15, FI)
mail.tamk.fi	MX	3 hours	10	smtp.tamk.fi
www.tamk.fi	A	5 minutes		193.167.71.207 (Tampere, 15, FI)

Kuva 7: Lisää www.tamk.fi:n liittyviä DNS tietoja

Internetissä tehtävien hakujen lisäksi on käytettävissä useita sovelluksia Windows- ja Unix/Linux-ympäristöissä. Käytettävissä on myös komentoriviltä ajettavia ohjelmia. (Klevinsky ym. 2002, 53; McClure ym.. 2012, 30; who.is 2012.)

Tiedonhakua voi tehdä myös IP-osoitteiden perusteella. Testaajalla on lokitiedoista tai verkkotunnusten perusteella tehdyistä hauista selvinnyt IP-osoitteita ja testaaja haluaa varmistua selvinneiden tietojen paikkansa pitävyydestä. IP-osoitteista vastaa ICANN:in alainen IANA (Internet Assigned Numbers Authority) ja sen alueelliset alaosastot (RIR). Niiden järjestelmä on rakennettu siten että vaikka testaaja suorittaa haun, IP-osoitteella väärän alaosaston tietokannasta, osaa järjestelmä kertoa oikean alaosaston. (IANA 2013.)

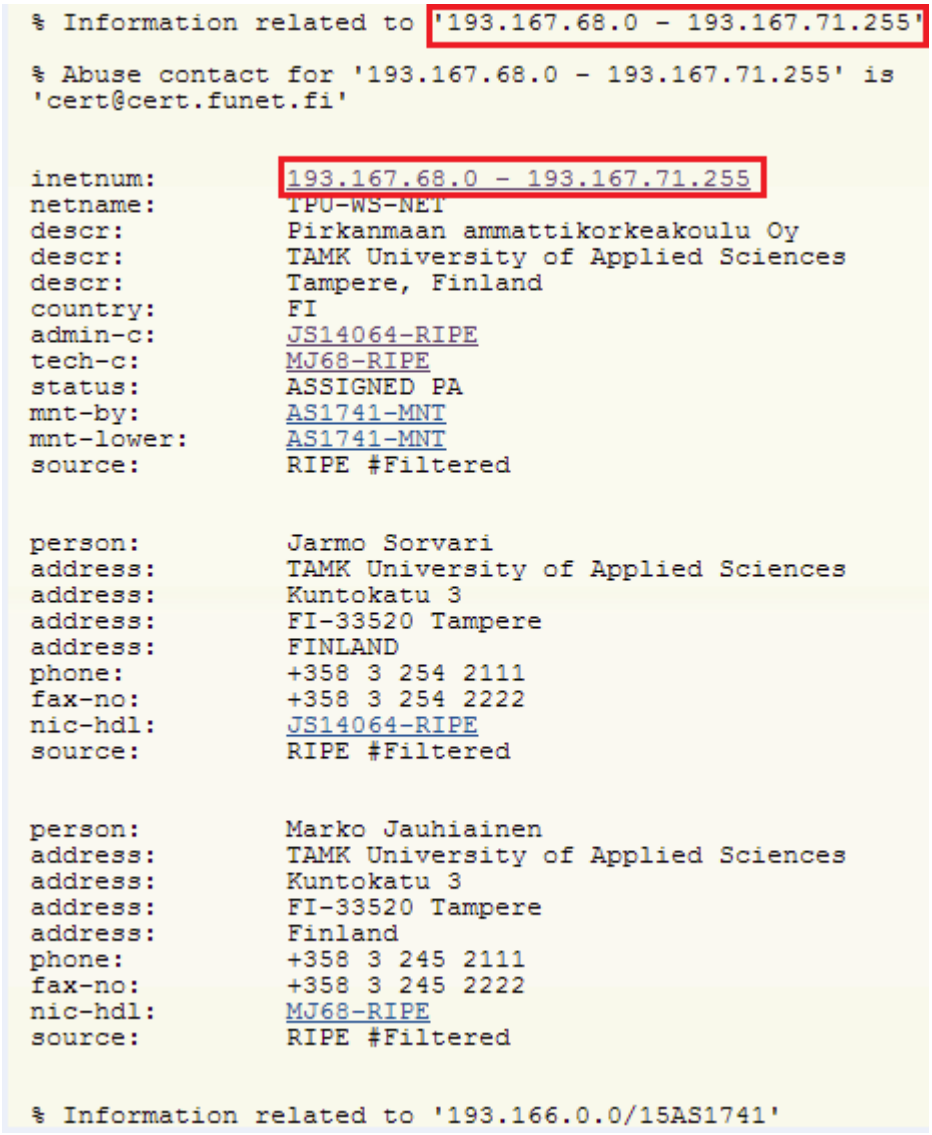
Kuvan 8 tulokset on saatu suorittamalla ARIN:n sivuilla (www.arin.net) haku who.is osoitteessa tehdyn haun tuloksista selvinneellä IP-osoitteella. ARIN vastaa pohjois-Amerikan IP-osoitteista. (McClure ym.. 2012, 28, 32 — 33; IANA 2013.)



Network	
NetRange	193.0.0.0 - 193.255.255.255
CIDR	193.0.0.0/8
Name	RIPE-CBLK
Handle	NET-193-0-0-0-1
Parent	
Net Type	Allocated to RIPE NCC
Origin AS	
Organization	RIPE Network Coordination Centre (RIPE)
Registration Date	1992-08-12
Last Updated	2009-03-25
Comments	These addresses have been further assigned to users in the RIPE NCC region. Contact information can be found in the RIPE database at http://www.ripe.net/whois
RESTful Link	http://whois.arin.net/rest/net/NET-193-0-0-0-1
See Also	Related organization's POC records.
See Also	Related delegations.

Kuva 8: arin.net:n hakutulokset

ARIN:n sivuilla tehdyssä haussa selvisi että käytetty IP-osoite kuuluu RIPE:lle (Réseaux IP Européens), joka hallitsee muun muassa Euroopan IP-osoitteita. RIPE:n www-sivuilla saa huomattavasti enemmän tietoja käyttämästään IP-osoitteesta tekemällä RIPEstat haun ja erillisen tietokantahaun. RIPEstat:n tietoihin sisältyy reititystietoja, DNS-tietoja sekä tietysti IP-osoite tietoja. RIPE:n tietokannasta (WHOIS) selviää se IP-osoite avaruus, johon haussa käytetty osoite kuuluu sekä useita yhteystietoja. Tietokantahaun tulokset löytyvät kuvasta 9. (McClure ym.. 2012, 32 – 33; RIPE Network Coordination Centre. 2013; IANA 2013.)



```
% Information related to '193.167.68.0 - 193.167.71.255'

% Abuse contact for '193.167.68.0 - 193.167.71.255' is
'cert@cert.funet.fi'


inetnum:        193.167.68.0 - 193.167.71.255
netname:        TPU-WS-NET
descr:          Pirkanmaan ammattikorkeakoulu Oy
descr:          TAMK University of Applied Sciences
descr:          Tampere, Finland
country:        FI
admin-c:        JS14064-RIPE
tech-c:         MJ68-RIPE
status:         ASSIGNED PA
mnt-by:         AS1741-MNT
mnt-lower:      AS1741-MNT
source:         RIPE #Filtered


person:         Jarmo Sorvari
address:        TAMK University of Applied Sciences
address:        Kuntokatu 3
address:        FI-33520 Tampere
address:        FINLAND
phone:          +358 3 254 2111
fax-no:         +358 3 254 2222
nic-hdl:        JS14064-RIPE
source:         RIPE #Filtered


person:         Marko Jauhiainen
address:        TAMK University of Applied Sciences
address:        Kuntokatu 3
address:        FI-33520 Tampere
address:        Finland
phone:          +358 3 245 2111
fax-no:         +358 3 245 2222
nic-hdl:        MJ68-RIPE
source:         RIPE #Filtered


% Information related to '193.166.0.0/15AS1741'
```

Kuva 9: RIPE:n tietokanta haun tulokset.

Pohjatietojen hankinnan jälkeen testaaminen voi muuttua aktiivisemmaksi. Aktiivinen tässä yhteydessä tarkoittaa sitä, että kohdejärjestelmää tutkitaan erilaisilla työkaluilla ja tiedot tulevat itse kohteesta, eivätkä ulkoisista lähteistä.

DNS vyöhykesiirto on lähes vanhentunut keino tietojen hankkimiseen kohdejärjestelmästä, mutta tämä ei tarkoita että se pitäisi unohtaa, sillä vieläkin löytyy väärin konfiguroituja DNS-palvelimia ja onnistuessaan vyöhykesiirto on merkittävä tiedonlähde. (McClure ym.. 2012, 36 – 37.)

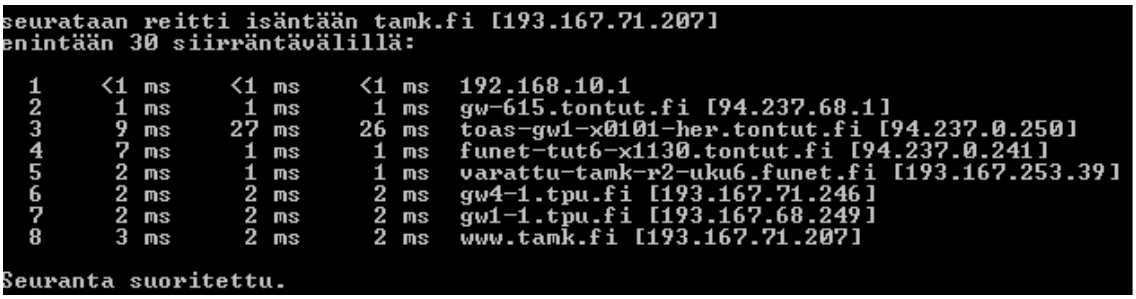
Vyöhykesiirto suoritetaan WHOIS-hauissa selvinneitä nimipalvelimia vastaan. Vyöhykesiirto pyytää nimipalvelimelta listauksen, jossa näkyy IP-osoitteet ja niitä vastaavat nimet. Vyöhykesiirron voi suorittaa useilla sovelluksilla tai Windows- ja Unix-

käyttöjärjestelmiin sisältyvällä nslookup komennolla. Vyöhykesiirron kohteena olevan nimipalvelimen pitää olla kyseisen vyöhykkeen valtuuttava palvelin. Tuloksia tutkiessa kannattaa muistaa, että nimipalvelimella välttämättä ole tietoja kaikista verkon laitteista. Tulosten kattavuuteen vaikuttaa DHCP:n käyttö verkon laitteissa ja se että käytetäänkö eri verkkotunnuksille eri nimipalvelimia. (Klevinsky ym. 2002, 54 — 56.)

Vyöhykesiirto saattaa olla kuitenkin estetty monessa paikassa, mutta tämä ei välttämättä estä saamasta DNS tietoja. On olemassa ohjelmia ja skriptejä, jotka käyttävät hyväkseen julkisen tiedon lähteitä (IANA, WHOIS), käänteisiä DNS hakuja tai yksinkertaisesti korvaavin keinoin hankkivat DNS tiedot. (McClure ym. 2012, 40; Mouton, W. 2013, 3.)

Kun tunnetaan nimet ja osoitteet, voidaan ryhtyä selvittämään sijaintia. Sijainnin kartoittaminen vie aikaa, mutta sen avulla saa käsityksen missä palvelimet ja muut tietokoneet sijaitsevat suhteessa verkon turvalaitteisiin. Kartoituksessa selviää myös, jos jotkin laitteet sijaitsevat eri osassa (segmentissä) verkkoa. Kartoittamisessa voi käyttää joko Unixin tai Windowsin komentoriviltä toimivaa traceroutea / tracertia tai VisualRoutea, joka esittää tulokset visuaalisessa muodossa. (Klevinsky ym. 2002, 58.)

Yksinkertaisimmillaan tulokset ovat melko selkokielisiä, kuten kuvasta 10 voi huomata.



Kuva 10: tracert:lla selvinnyt reitti osoitteeseen tamk.fi

Aikaisempien tulosten ja kuvan 10 esittämien tulosten perusteella, voidaan päätellä että kohteet 5 – 8 ovat laitteita, jotka kuuluvat tamk:lle. Todellisuudessa tilanne on huomattavasti monimutkaisempi, sillä verkossa saattaa olla useita reittejä kohteeseen ja reittien varsilla saattaa olla kuormantasauslaitteita. Pääsylistat (ACL) saattavat myös sekoittavat tuloksia, sillä niiden yksityiskohdat vaihtelevat laitteesta laitteeseen. Tästä johtuen toiset laitteet päästävät tracert:n läpi, toisten estäessä sen kulun. (McClure ym. 2012, 43 — 45; Vesaria Network Security Specialists 2013.)

Kartoittamisen tulokset vaativat hieman tulkintaa, jotta niistä on hyötyä testaajalle. Yksi tärkeä tarkkailun kohde on kartoitukseen käytetyn ohjelman ICMP-pakettien reitti. Jos useaan eri kohteeseen matkaava paketti käyttää samaa reittiä, on se ensimmäinen merkki verkon osien rajoilla sijaitsevista laitteista. Tällaisen laitteen olemassaolo varmistuu, jos usealla paketilla on ennen kohdettaan sama hyppy. Jos paketteja ei voida havaita enää tietyn pisteen jälkeen, on kyseessä todennäköisesti palomuuri tai liikennettä suodattava reititin. Riippuen kohteesta kyseessä voi olla myös kuormantasauslaite tai muu liikenteen kulkuun vaikuttava laite. Kartoituksen aikana voi huomata, että jotkin paketit ottavat vaihtoehtoisen reitin johonkin kohteeseen. Tällöin voi olla kyse jonkin projektin aikana paikalleen unohtuneista kytkennöistä. Testaajan kannalta tämä on hyvä, sillä näillä kytkennöillä monesti kierretään turvalaitteita tai muuta tietoturvallisuuteen liittyvää toiminallisuutta ja jätetään näin aukko verkkoon. (Klevinsky ym. 2002, 58 — 59.)

3.2.2 Skannaus

Aiemmissa testauksen vaiheissa on selvinnyt joitakin IP-osoitteita, joita voi käyttää skannauksen aloittamiseen. Skannaus paljastaa lisää osoitteita, joiden pohjalta skannausta voidaan laajentaa. Pelkillä IP-osoitteilla ei tee juuri mitään myöhemmässä testauksessa, kun ei tiedetä ovatko osoitteet oikeasti toiminnassa. Siksi skannaus aloitetaan selvittämällä mitkä kohteen osoitteet ovat toiminnassa. Tähän tarkoitukseen voisi käyttää Windowsista ja UNIX:sta löytyvää komentorivisovellusta ping, mutta se olisi vaivalloinen käyttää ja sovelluksen suorittaminen on rajoitettu ICMP (Internet Control Message Protocol)-paketteihin. On olemassa sovelluksia, jotka osaavat ICMP-pakettien lisäksi käyttää ARP (Address Resolution Protocol)-, TCP (Transmission Control Protocol)- tai UDP (User Datagram Protocol)-paketteja. (Klevinsky ym. 2002, 57; McClure ym. 2012, 48.)

ICMP pingillä on kuitenkin muutama käyttökelpoinen ominaisuus sen käyttämien viestityyppien ansiosta. ICMP pingiä käyttäessä kyse on *echo reply* ja *echo request* viesteistä. Kaksi muuta käyttökelpoista viestiä ovat *Timestamp*, jolla saa selville kohteen järjestelmä ajan, ja *Address mask*, joka puolestaan kertoo kohteen aliverkkomaskin. (McClure ym. 2012, 52; Microsoft 2013.)

Testaajan ollessa samassa verkkosegmentissä kohteen kanssa ARP-paketteihin perustuva menetelmä vie vähiten aikaa ja luo vähiten liikennettä verkkoon. ARP skannauksessa lähetetään ARP-pyyntö jokaiseen osoitteeseen tietyn aliverkon alueella ja osoite katsotaan toimivaksi, jos pyyntöön vastataan. ARP-skannauksella voidaan myös todeta sellaisten osoitteiden toimivuus, jotka ovat paikallisen palomuurin takana, joka puolestaan saattaa suodattaa muita skannaukseen soveltuvia paketteja. (McClure ym. 2012, 48 — 49; The Sprawl 2009.)

Monet sovellukset voivat yhdistää toiminnassa olevien kohteiden tunnistamisen TCP- tai UDP-pakettien avulla, ja porttiskannauksen, jonka tavoitteena on tunnistaa mitkä palvelut toimivat avoimien porttien takana. Testin ollessa tyypiltään ennalta ilmoitettu voidaan kaikki portit skannata, koska havaituksi tuleminen ei haittaa. Testaustyypistä huolimatta kannattaa testaajan jakaa skannattavat portit useaan erään, joko porttinumeroiden tai protokollan mukaan. Skannaamalla portit useassa erässä vältetään kuormittamasta kohde verkkoa. (McClure ym. 2012, 61 — 64; Klevinsky ym. 2002, 60 — 61.)

Testaajan tulisi kehittää itselleen eräänlainen ”pohjalista” porttiskannausta varten, jota voisi käyttää mihin tahansa järjestelmään ja muokata sitten tilanteen mukaan. Tälläisen listan työstämisen voi aloittaa jonkin sovelluksen käyttämästä listasta tai jostakin muusta valmiista listasta. Lista kehittyy testaajan kehittyessä sekä kunkin testauksen tiedonkeräyksen tuloksena. Valtaosa porttiskannaus tyypeistä on erilaisia TCP-pohjaisia skannauksia ja jotkin niistä toimivat vain tietynlaisiin kohteisiin, kuten esimeriksi UNIX-järjestelmiin. Oikeanlaisen skannaustavan valintaan vaikuttaa myös se että missä testauksen vaiheessa ja millaisin oikeuksin skannausta suoritetaan. Eri skannaustavat, vaikkakin periaatteessa tekevät samaa asiaa, tavasta riippuen selvittävät porttien tilan eri tavalla. (Klevinsky ym. 2002, 61; McClure ym. 2012, 62 — 63.)

3.2.3 Käyttöjärjestelmän tunnistaminen

Käytössä olevien palveluiden lisäksi on tunnistettava käyttöjärjestelmä jonka päällä palveluita ajetaan. Tunnistamiseen on kaksi lähestymistapaa: aktiivinen ja passiivinen. (McClure ym. 2012, 72 — 73.)

Aktiivisessa lähestymistavassa tunnistaminen perustuu porttinumeroihin ja kokenut testaaja voisikin porttiskannauksen perusteella esittää arvauksen käyttöjärjestelmästä. Ar-

vausten luotettavuus on kuitenkin heikko, sillä porttinumerossa saattaa esiintyä päällekkäisyyksiä ja numeroita on voitu vaihtaa. (McClure ym. 2012, 73.)

Aktiivisessa lähestymistavassa käytettävän työkalun tunnistus perustuu TCP ja ICMP pakettien ominaisuuksien manipulointiin, jolla pyritään saamaan tietynlainen vastaus kohteelta. Tuloksen perusteella pystytään melko pitkälle yksilöimään mistä käyttöjärjestelmästä on kyse. Tunnistus on sitä tarkempi mitä enemmän kohteessa on portteja auki, mutta vaikka kohteessa ei olisi yhtään porttia auki, voi esimerkiksi Nmap-ohjelma suorittaa arvauksen käyttöjärjestelmästä. (McClure ym. 2012, 74 — 76.)

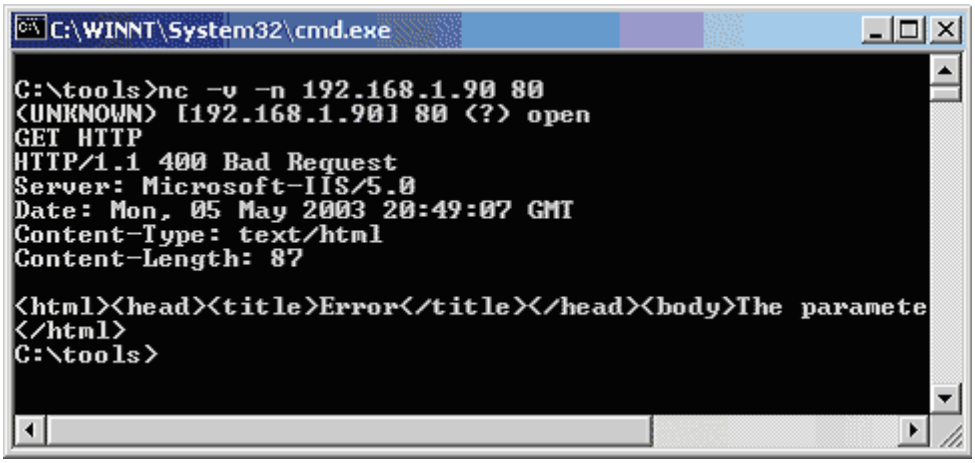
Aktiivisen tunnistamisen haittapuolena on kuitenkin että se herkästi laukaisee IDS (Intrusion Detection System)-järjestelmät. Passiivisessa tunnistamisessa kohteeseen ei lähetetä paketteja, vaan tunnistaminen perustuu nimen mukaisesti verkon liikenteen passiiviseen tarkkailuun. Passiivinen tunnistaminen kuitenkin edellyttää, että testaaja sijaitsee keskeisellä paikalla suhteessa verkon liikenteeseen ja pystyy yhdistämään tietokoneensa porttiin, joka sallii pakettien kaappaamisen. (McClure ym. 2012, 77.)

Passiivinen tunnistaminen perustuu pakettien TTL (Time To Live)-, Window size- ja DF (Don’t Fragment)-arvoihin. Menetelmän heikkoutena on kuitenkin että jos tarkkailtu liikenne tulee sovelluksista, jotka muodostavat omia pakettejaan, saattavat tarkkailtavat ominaisuudet muuttua käyttöjärjestelmän arvoista. Kumpaakin lähestymistapaan vaikuttaa se tosiasia että käyttöjärjestelmän käyttämiä arvoja voidaan muuttaa. (McClure ym. 2012, 78 — 79.)

3.2.4 Haavoittuvuuksien analysointi

Monia haavoittuvuuksia voi etsiä ja löytää jo tähän mennessä hankituilla tiedoilla, mutta kovin tarkkoja tuloksia ei välttämättä saada. Sovellusten haavoittuvuudet usein muuttuvat versiosta toiseen, joten niiden tarkkojen versionumeroiden selvittäminen on tärkeää testaamisen kannalta. (McClure ym. 2012, 85 — 86.)

Www-palvelimien version saa usein selville myös käyttämällä hyväkseen tunnisteen kaappausta (Banner). Tunnisteen kaappaus tapahtuu ottamalla telnetyhteys johonkin www-osoitteeseen porttinumerolla 80 tai esimerkiksi netcat sovelluksella, jonka toiminnasta esimerkki kuvassa 11.



Kuva 11: Netcat sovelluksen käyttö tunnisteen kaappaamisessa. (Reed, B. 2011)

tunnisteen kaaappaus toimii myös muihinkin yleisiin palveluihin, kuten esimerkiksi FTP:hen (File Transfer Protocol) tai SMTP:hen (Simple Mail Transfer Protocol). (McClure ym. 2012, 90 — 91; Reed, B. 2011.)

Haavoittuvuuksia voi etsiä käsin Internetin haavoittuvuustietokannoista, mutta myös tähän tarkoitukseen on saatavilla sovelluksia, kuten esimerkiksi Nessus tai Nmap. Joidenkin lähteiden mukaan Nessus olisi suhteellisen epäluotettava sovellus käytettäväksi testaamiseen. (McClure ym. 2012, 87 — 89; Saarelainen, A. 2013.)

Jotkin palvelut ovat hyödynnettävissä hyökkäyksessä aivan sellaisenaan, olettaen että niihin liittyvät portit ovat tiedonkeruussa selvitetty auki oleviksi. Ihmisten huolimattomuus tai tietämättömyys joidenkin palveluiden käytössä altistaa kohteen näin ollen hyökkäyksille näiden palveluiden kautta.

FTP väärin konfiguroituna on otollinen kohde hyökkääjälle, sillä sen haavoittuvuuden löytää hyvin yksinkertaisella tavalla: ottamalla yhteys FTP-palvelimeen. Pelkkä yhteyden ottaminen saattaa paljastaa käytössä olevan FTP-sovelluksen nimen ja version. Samalla kertaa on helppo testata salliiko kyseinen FTP-palvelin anonyymit kirjautumiset, joka itsessään on jo hyödynnettävissä haavoittuvuutena. (McClure ym. 2012, 92 — 93.)

Telnet tunnetusti lähettää käyttäjätunnuksen ja salasanan selkokielisenä tekstinä. Tästä syystä sen käyttöä vältetään. Mainittakoon kuitenkin esimerkkinä, että Ciscon laitteita on mahdollista tunnistaa pelkästään niiden antaman kirjautumiskehotteen perusteella,

tämän haavoittuvuuden hyödyntäminen kuitenkin edellyttää, että kohde laitteessa on Telnet palvelu päällä. (McClure ym. 2012, 94 — 95.)

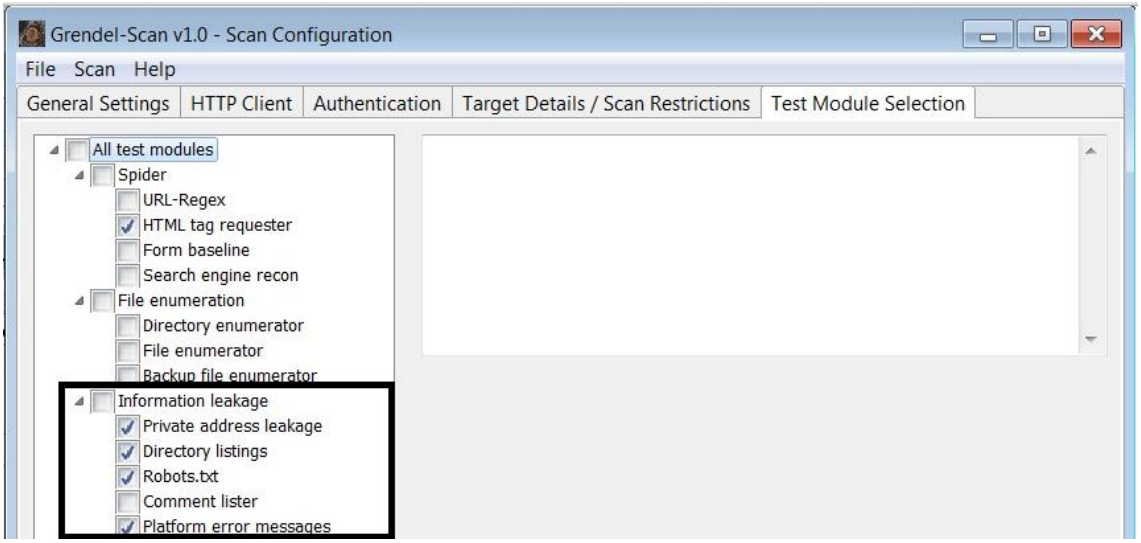
SMTP:n haavoittuvuus piilee sen komennoissa ja käyttäjänimissä. Monessa organisaatiossa käyttäjänimet ovat samat kuin sähköpostiosoitteen alkuosa ja käyttäjänimet muodostetaan monesti jonkin logiikan mukaan. Testaaja voi päättelemällä selvittää kyseisen logiikan ja näin muodostaa itselleen listan todennäköisistä käyttäjänimistä. Testaaja voi varmistua näiden käyttäjänimien toimivuudesta ottamalla yhteyden asianmukaiselle palvelimelle esimerkiksi telnet tai netcat ohjelmalla. Kuvassa 12 on hyödynnetty SMTP:n komentoja vrfy-skriptin avulla. (McClure ym. 2012, 96; Penetration Testing Lab 2012.)

Kuva 12: SMTP:n haavoittuvuuden hyödyntäminen vrfy-skriptin avulla (Penetration Tesing Lab 2012)

TFTP:en käyttö on harvinaista sen tietotuvattomuuden takia, mutta siitä huolimatta sitä käytetään Ciscon kytkimien, reitittimien tai VPN keskittimien konfiguraatioiden siirtämseen. Riippuen testauksen parametreista on TFTP otollinen tietolähde koskien verkonlaitteita. (McClure ym. 2012, 102 — 103.)

WWW-sivujen koodin joukkoon saattaa olla piilotettuna esimerkiksi salasanoihin liittyvää tietoa. Tietojen hankkiminen www-sivuista ei päällisin puolin juurikaan eroa tunnisteen kaappauksesta, ellei kohde sivu käytä SSL:ää. Kuvassa 13:sta on etsitty tietoa

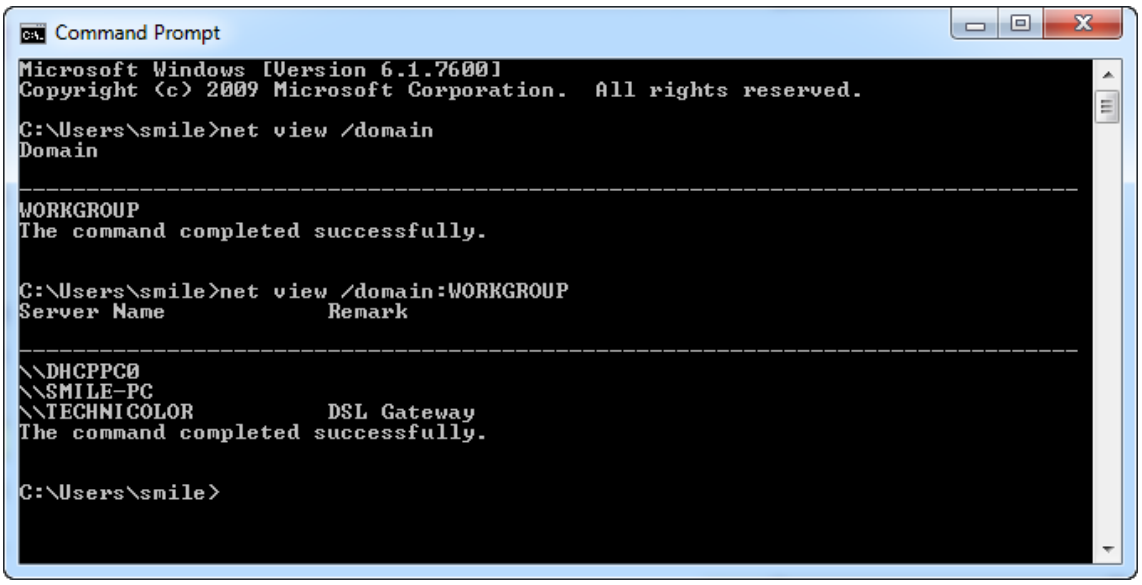
WWW-sivujen koodin joukosta siihen tarkoitetulla sovelluksella (kohta ”Information leakage”). (McClure ym. 2012, 104 — 105.)



Kuva 13: Grendel-Scan sovelluksella voi etsiä tietoa WWW-sivujen koodin joukosta. (DragonJAR 2009.)

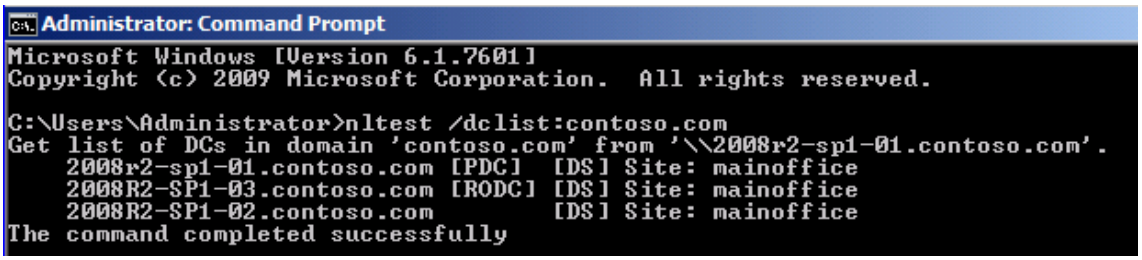
Tietyt Windowsit saattavat käyttää RPC (Remote Procedure Call) Port Mapper ohjelmaa, jonka kautta voidaan saada oleellisia tietoja kohteen sovelluksista ja palveluista sekä niihin liittyvistä IP-osoitteista. Microsoftilta itseltään löytyy työkalu (Resource Kit, epdump) näiden tietojen hankkimiseen, mutta tulokset eivät ole kovin selkeät ja yksiselitteiset. Testaajan käyttöön löytyy myös skriptejä ja graafisia sovelluksia, jotka tekevät saman asian ja antavat selkeämpiä tuloksia. (McClure ym. 2012, 108 — 109; Hackit 2013.)

NetBIOS:n nimipalvelua (UDP 137) ei ole välttämättä tarvinnut enää käyttää DNS:n yleistymisen myötä, mutta siitä huolimatta se on lähes jokaisessa Windows-versiossa oletuksena päällä. NetBiosista saa tietoja melko helposti, jopa käyttöjärjestelmien omilla työkaluilla. Kuvassa 14 on esitetty komennot, jotka listaavat toimialueen johon tietokone kuuluu ja sen jälkeen kaikki toimialueeseen kuuluvat tietokoneet. (McClure ym. 2012, 108 — 109; Klevinsky ym. 2002, 99 — 100.)



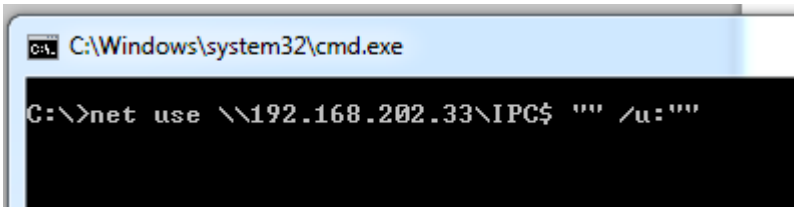
Kuva 144: net view:n käyttö NetBIOS:n hyödyntämisessä (University Of South Wales 2013.)

Kuvassa 15 nähdään kuinka nltest-komennolla saadaan selville tietyllä toimialueella sijaitsevat DC:t (Domain Controller).



Kuva 155: nltest sovelluksen käyttö NetBIOS:n hyödyntämisessä (Microsoft 2013.)

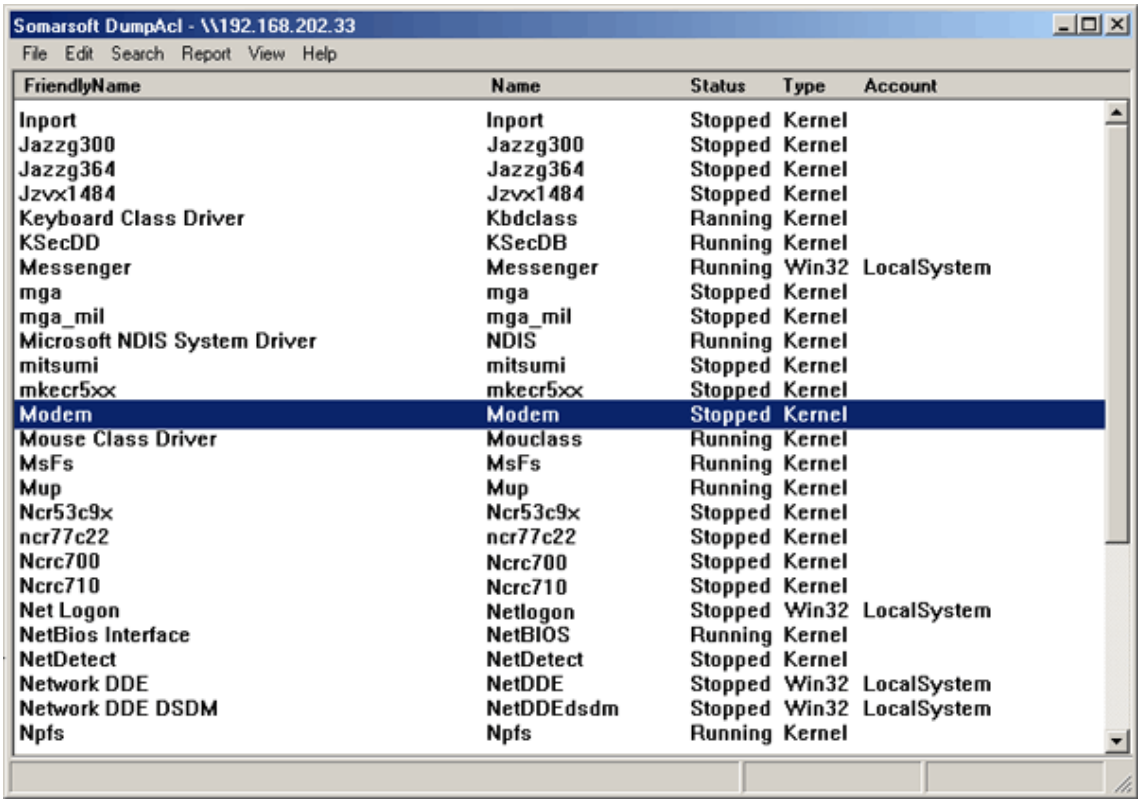
NetBIOS istunnossa piilee haavoittuvuus, josta puhutaan myös nimellä null istunto / anonymous yhteys. Haavoittuvuuden muodostaa Microsoftin SMB (Server Message Block), johon puolestaan perustuu Windowsin tiedostojen ja tulostimien jako. Tietojen saaminen SMB:stä onnistuu ottamalla yhteys piilotettuun jakoon IPC$ ja se tapahtuu *net use* komennolla, jolla Windowsissa yhdistetään normaaliin verkkojakoon, kuten kuvasta 16 voi nähdä. Ensimmäiset lainausmerkit kertovat että käytetään tyhjää salasanaa ja jälkimmäinen määrittää käyttäjätunnukseksi anonymous.



Kuva 166: IPC$ jakoon yhdistäminen *net use* komennolla

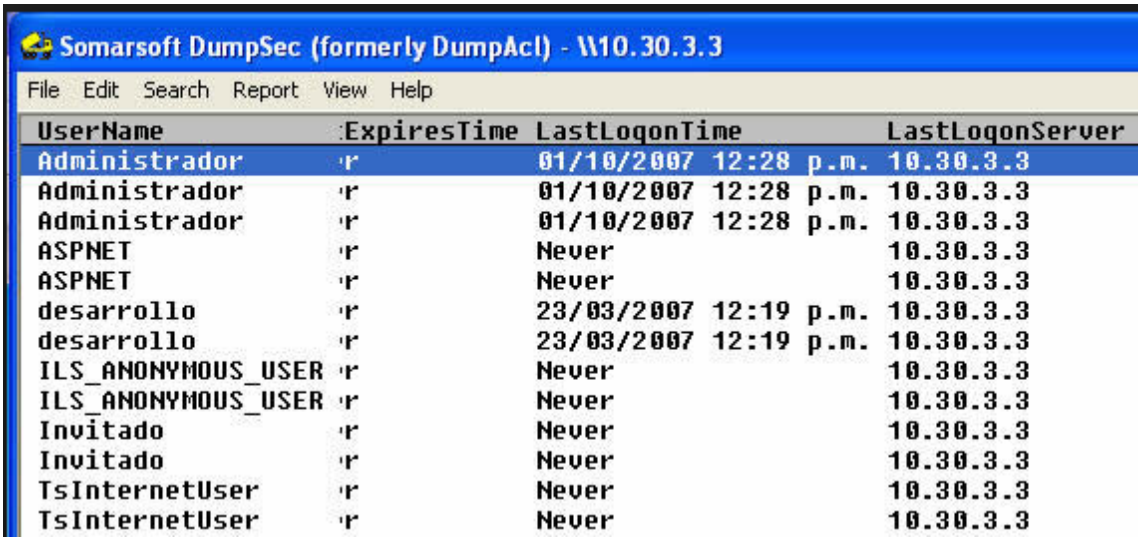
Vaihtoehtona komentokehotteelle on useita graafisia sovelluksia. Yhteyden muodostettuaan tietoa tiedostojaoista voi kerätä aiemmin mainitulla *net view*-komennolla. Nltest-komennolla voi null-yhteyden muodostuksen jälkeen hankkia tietoja muistakin toimialueista kuin siitä, johon on luonut yhteyden. (Klevinsky ym. 2002, 100; McClure ym. 2012, 115 — 116, 120; Microsoft 2013; Minasi, M. 1998.)

Periaatteessa on mahdollista saada tietoja rekisteristäkin, mutta oletuksena Windows sallii vain ylläpitäjien pääsyn rekisteritietoihin. Normaali tilanteessa null-yhteyden kautta rekisteriin ei pääse käsiksi. Poikkeuksia kuitenkin löytyy, jotka mahdollistavat joidenkin tietojen saamisen rekisteristäkin. Monilla sovelluksilla saattaa olla versionumero asennuspolussa. Myös pelkällä sovelluksen nimellä pääsee alkuun haavoittuvuuksien etsinnässä. Kuvassa 17 on esitetty rekisteritietojen hankinnan tulokset DumpAcl (nyk. DumpSec) sovelluksella. (McClure ym. 2012, 118 — 119; Microsoft 2013; Corelan Team 2008.)



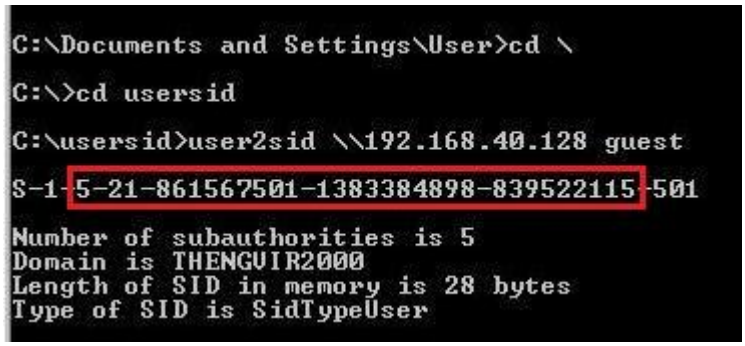
Kuva 177: DumpAcl sovelluksen rekisteristä hankkimat tiedot (lib.qrz.ru 2013.)

Jakojen ja toimialueiden lisäksi null-yhteydestä on mahdollista saada käyttäjänimet sekä muuta niihin liittyvää tietoa, jotka Windows antaa melkoisen helposti. Kuvassa 18 kyseiset tiedot on hankittu DumpSec:llä.



Kuva 188: Käyttäjänimien hankinta DumpSec:llä (DragonJAR 2008.)

Toisena vaihtoehtona on käyttää sovelluksia user2sid ja sid2user, joissa käyttäjätunnusten selvittäminen perustuu SID (Security IDentifier)- ja RID (Relative IDentifier)-numeroihin. Kuvassa 19 näkyy kuinka user2sid:ä on käytetty SID-numeron selvittämiseksi. Kuvaan merkitty osio on SID-numero. (McClure ym. 2012, 120 — 122; Microsoft 2013.)

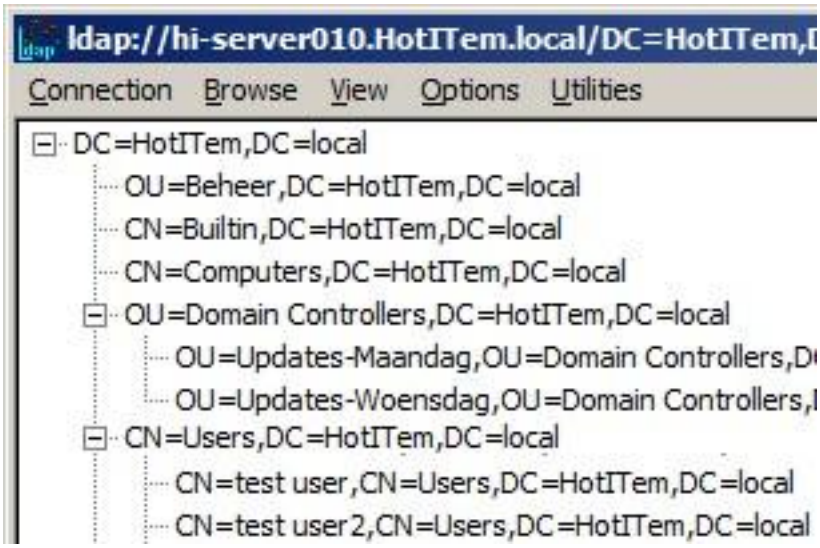


Kuva 19: user2sidin käyttö SID-numeron selvittämiseksi (Bangash Hacker 2013.)

Kuvassa 20 käytetään sid2useria selvittämään tietyn tyyppisen käyttäjän käyttäjänimi. Ensimmäinen merkitty numerosarja on edellisessä kuvassa näkyvä SID-numero ja jälkimmäinen numero on pääkäyttäjän tunnusta vastaava RID-numero.

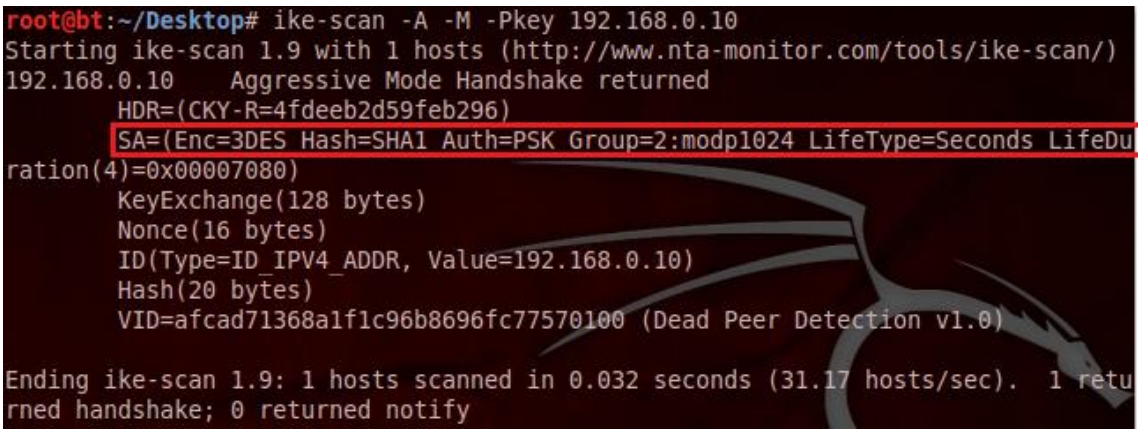
Kuva 190: sid2userin käyttö pääkäyttäjän tunnuksen selvittämiseksi (Bangash Hacker 2013.)

Microsoftin AD:hen (Active Directory) ja erityisesti siihen liittyvästä LDAP:sta (Lightweight Directory Access Protocol) saa hankittua tietoja käyttäjistä ja käyttäjäryhmistä. Tämä on kaiken lisäksi AD:n ja LDAP:n normaalia toimintaa ja Windowsille löytyy tarkoitusta varten virallinen sovellus, Active Directory Administration Tool (ldp.exe). Tämän sovelluksen avulla otetaan yhteys DC:hen portin 389 tai portin 3268 kautta. Yhteyden muodostuksen jälkeen sovellukselle annetaan toimialueen juuren tiedot. Esim. dc=esimerkki, dc=fi. Yhteyden muodostuksen ja DC:n tietojen antamisen jälkeen saadaan käyttöön AD:stakin tuttu puunäkymä, josta esimerkki kuvassa 21. (McClure ym. 2012, 140 — 142.)



Kuva 201: ldp.exe sovelluksen avulla saa hankittua käyttäjänimiä (Gerard, N. 2009.)

IPSec (Internet Protocol Security) VPN ja siihen liittyvä IKE (Internet Key Exchange) muodostavat yhdessä suhteellisen tietoturvallisen yhdistelmän liikenteen salaamiseen. IPSec VPN:n olemassaoloakin on hyvin hankala paljastaa tavallisen porttiskannauksen keinoin, sillä IPSec:n luonteeseen kuuluu, että väärin muodostetut paketit hylätään kaikessa hiljaisuudessa. Aukoton tämäkään ratkaisu ei ole kuten kuvasta 22 voi nähdä. Merkityllä alueella on salaukseen liittyvät yksityiskohdat. (McClure ym. 2012, 153 — 154; Rebootuser 2013.)



Kuva 212: ike-scanin käyttö VPN yhteyden salauksen murtamisessa (Rebootuser 2013.)

Ike-scan sovelluksen mukana tulee myös psk-crack niminen sovellus, jolla voidaan murtaa salauksen avain, jos se selvisi ike-scanin ajon aikana. (McClure ym. 2012, 153 — 154.)

3.3 Hyökkäys

Hyökkäykset voidaan jakaa kahteen kategoriaan. **Todentamattomat hyökkäykset**, joissa hyödynnetään aiemmin hankittuja tietoja. **Todennetut hyökkäykset** perustuvat ensiksi mainittujen tuloksiin. Todentamattomissa hyökkäyksissä hyökkääjä (testaaja) sijaitsee vielä järjestelmän ulkopuolella. Todennetuissa hyökkäyksissä ollaan jo järjestelmän sisällä, mutta oikeuksia tarvitaan lisää. (McClure ym. 2012, 161.)

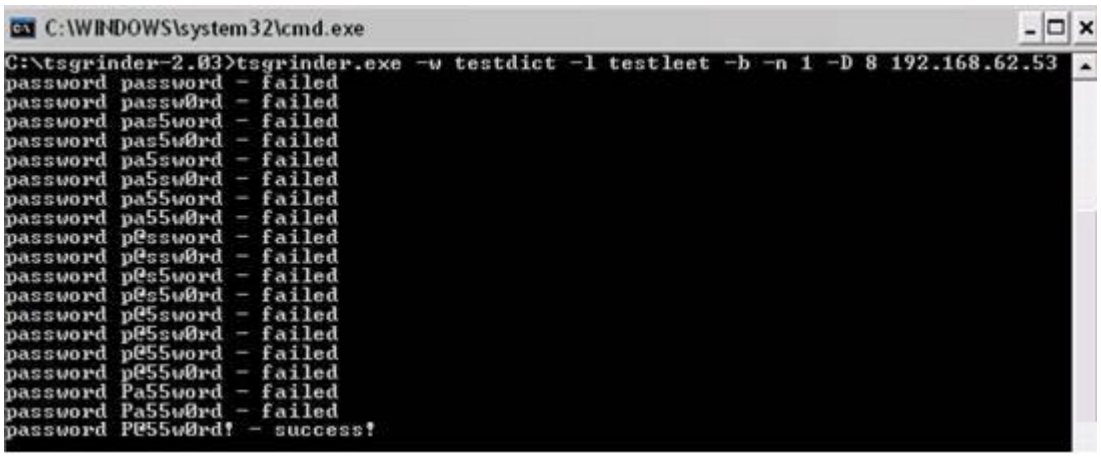
3.3.1 Todentamattomat hyökkäykset

Todentamattomat hyökkäykset voidaan edelleen jakaa neljään osa-alueeseen: Todennuksen väärennys, Verkon palvelut, Asiakasohjelmien haavoittuvuudet ja Laiteajurit. (McClure ym. 2012, 162.)

Todentamisen väärentäminen tarkoittaa salasanan arvaamista sanaston avulla, sen murtamista menetelmillä, jossa käytetään raakaa laskennallista voimaa (brute force) tai käyttämällä mies välissä hyökkäystä (man in the middle). Testaajan ollessa vielä järjestelmän ulkopuolella todentamiseen käytetään arvaamista ja monesti sen kohteena on SMB-palvelu, MSRPC(Microsoft Remote Procedure Call), TS (Terminal Services), SQL(Structured Query Language) sekä Sharepoint. Monissa Windows-versioissa SMB on kuitenkin oletuksena estettynä, mutta poikkeuksena on kuitenkin ne koneet, jotka

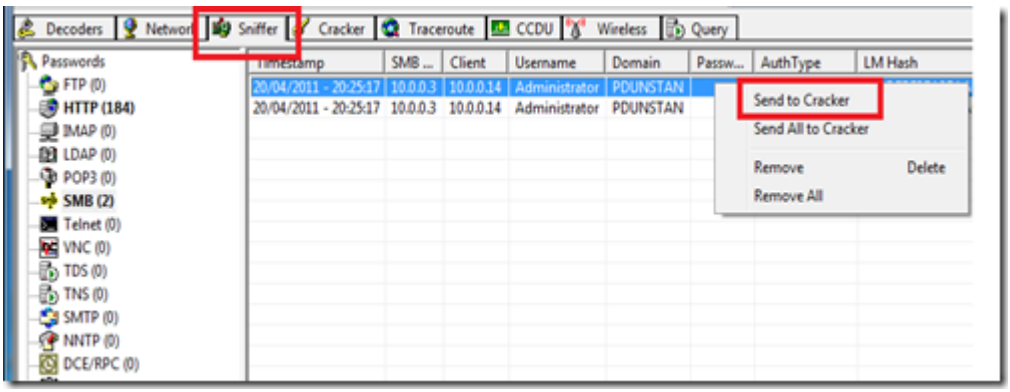
toimivat DC:nä. Kun yhteys SMB:hen on saatavilla, yksinkertaisinta on yrittää ottaa yhteys johonkin jakoon, kuten esimerkiksi null-yhteyden yhteydessä mainittuun IPC$:iin ja arvata sopivalle käyttäjätunnukselle salasanaa. Todentamistietojen selvittäminen on kuitenkin nopeampaa ja tehokkaampaa, jos sen apuna käyttää jonkinlaista sanastoa ja arvailun suorittaa jollakin skriptikielellä. Tarkoitukseen löytyy myös valmiita sovelluksia. (McClure ym. 2012, 162 — 164.)

TS:n kautta salasanan selvittäminen onnistuu valmiilla sovelluksella (tsgrinder). Tsgrinder selvittää oletuksena pääkäyttäjän (Administrator) salasanaa omalla sanastollaan, mutta muidenkin käyttäjien salasanan selvittäminen on mahdollista. TSgrinder toimii parhaiten vanhempia Windows-versioita vastaan ja vanhempien RDC versioiden kanssa. Kuvassa 23 on esimerkki tsgrinder ohjelman käytöstä. Kuvan esittämässä tilanteessa on käytetty muuta kuin tsgrinder ohjelman omaa sanastoa. (McClure ym. 2012, 164 — 165; Roth, M. 2006.) Kuvaa on tiivistetty alkuperäisestä.



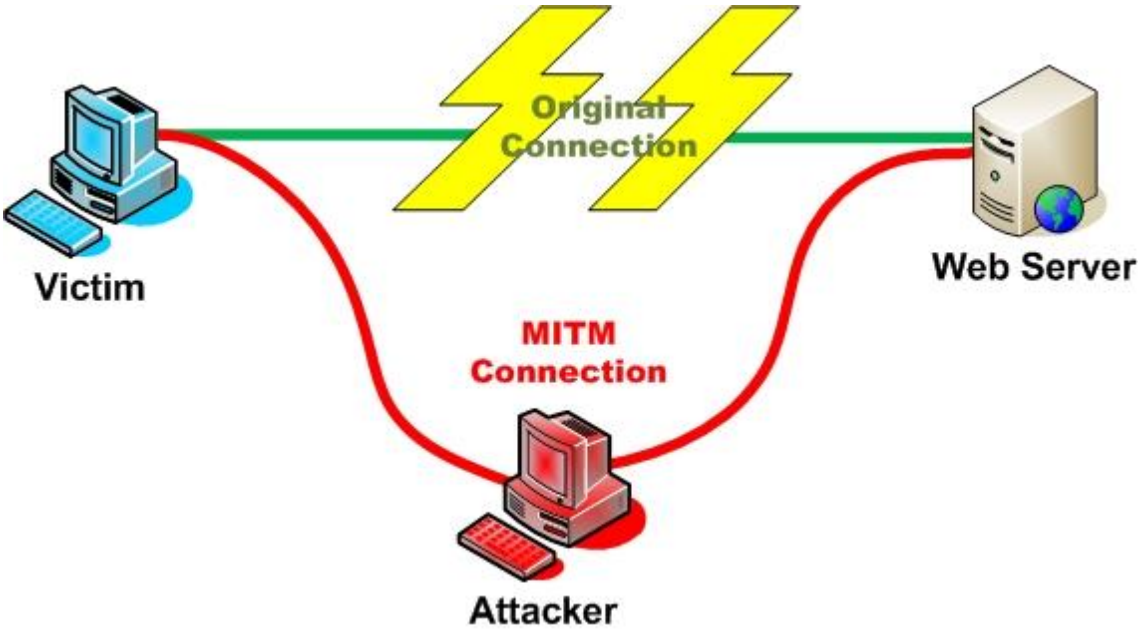
Kuva 223: tsgrinderin käyttö omalla sanastolla (Roth, M. 2006.)

Arvailua houkuttelevampi keino on kaapata tieto verkkoliikenteestä. Windows-järjestelmiä vastaan hyökätessä tämä tarkoittaa LM (LAN Manager), NTLM (NT LAN Manager) tai Kerberokseen liittyvän liikenteen kaappaamista. LM todentamisprotokollana on vanhentunut, mutta sitä saattaa edelleen löytyä joistakin verkoista. Sittemmin Windowsissa on siirrytty NTLM protokollaan. Saatavilla on useita sovelluksia tähän tarkoitukseen, mutta useassa sovelluksessa kaapatut tiedot pitää siirtää erilliseen salasananmurtosovellukseen. Kuvassa 24 on esitetty Cain-sovellus, joka voi kaapata liikennettä ja murtaa salasanan. (McClure ym. 2012, 170 — 172; Dunstan, P. 2011.)



Kuva 234: Cain:lla voi kaapata verkon liikennettä ja murtaa salasanan (Dunstan, P. 2011.)

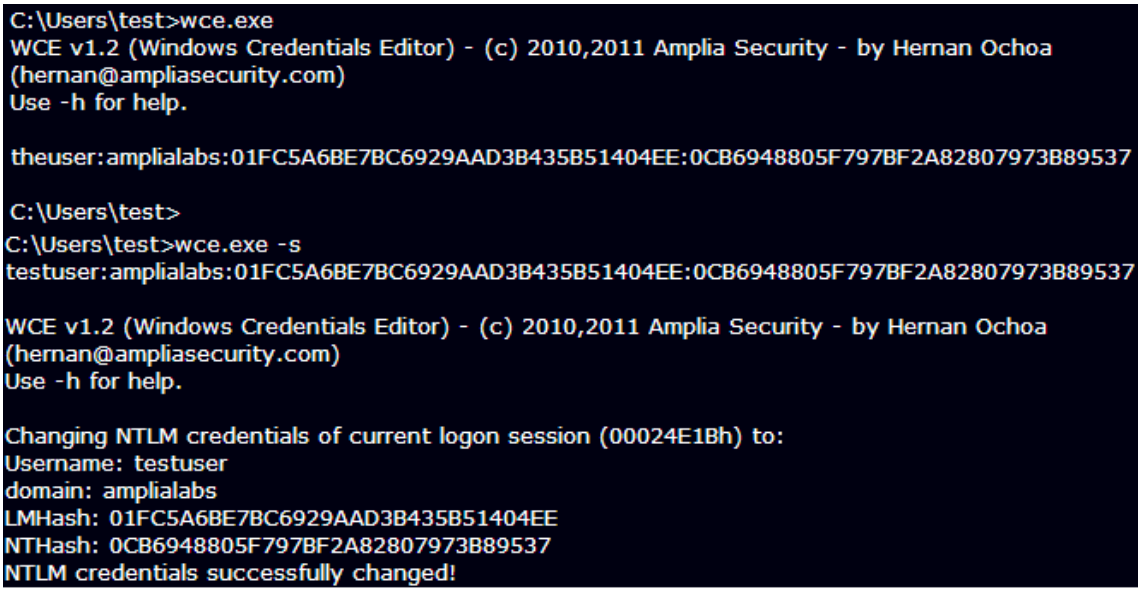
Mies välissä hyökkäyksissä hyökkääjä asettuu esimerkiksi palvelimen ja käyttäjän väliin. Hyökkääjä ohjaa liikenteen kulkemaan oman laitteensa kautta ja pystyy lukemaan sitä. Edellä mainitusta Cain-sovelluksesta löytyy mahdollisuus mies välissä hyökkäykseen. Kuvassa 25 on esitetty mies välissä hyökkäys. (McClure ym. 2012, 173 — 174; OWASP 2009.)



Kuva 245: Mies välissä hyökkäys (OWASP 2009.)

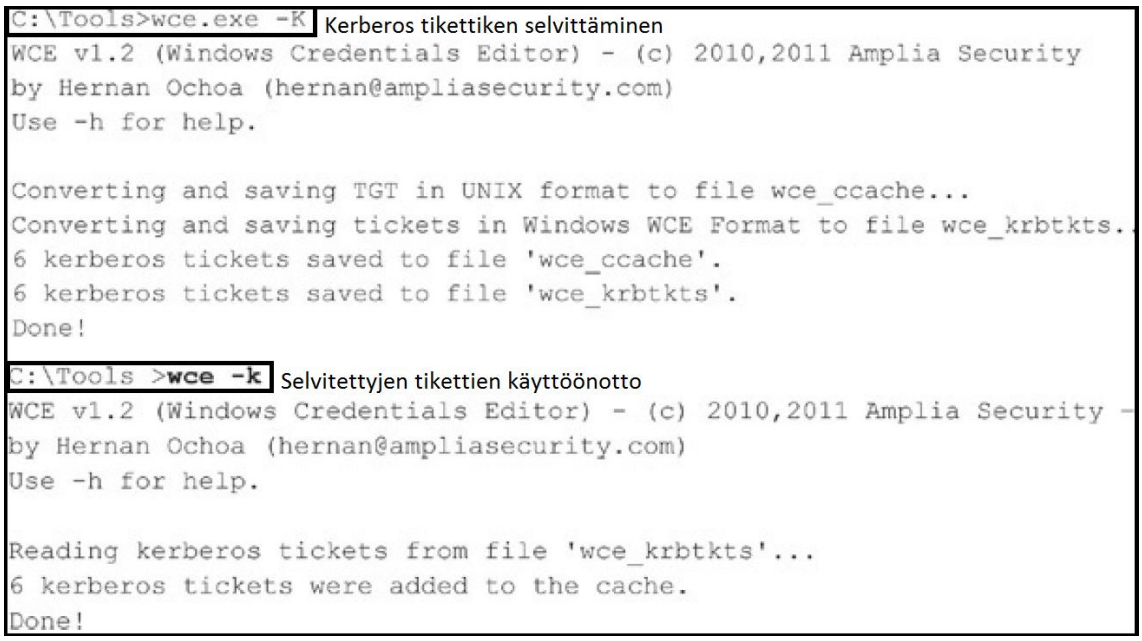
Pass-the-Hash hyökkäyksessä pääsy järjestelmään saadaan salasanaan liittyvän tarkisteen avulla, joten salasanan arvaaminen tai selvittäminen on tarpeetonta. Pass-the-Hash hyökkäys toimii sellaisia palveluita vastaan, jotka käyttävät todentamiseen LM:ää tai NTLM:ää. On olemassa tekniikoita, joissa käytetään tarkisteita ja Windows-käyttöjärjestelmästä löytyviä sovelluksia, kuten esimerkiksi Internet Exploreria, ottamaan yhteys sellaisiin palveluihin, jotka käyttävät NTLM todentamista. Kuvassa 26 on

käytetty WCE nimistä sovellusta NTLM tarkisteen selvittämiseen ja käyttöönottoon. Tämä keino kuitenkin vaatii, että testaajalla on käytössään paikallisen pääkäyttäjän tunnukset. (McClure ym. 2012, 175 — 176; Amplia Security 2012.)



Kuva 26: WCE:n käyttö NTLM tarkisteen selvittämiseksi ja käyttöönottamiseksi (Amplia Security 2012.)

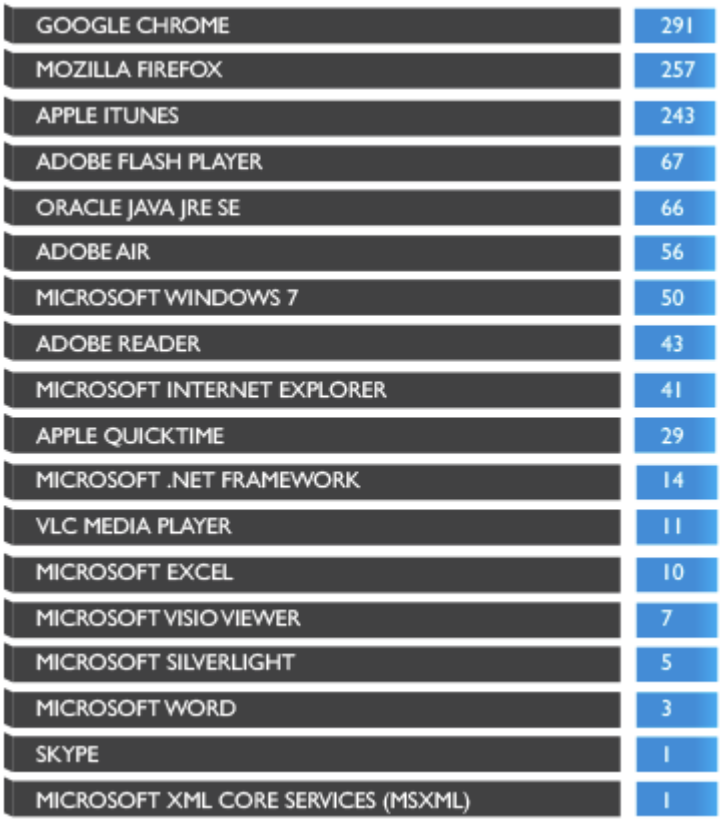
Kerberos todennuksen käyttämien tikettien hankkiminen pääsyn saamiseksi kohdejärjestelmään on hyvin samanlainen kuin pass-the-hash. Kun yhdelle laitteelle on pääsy kohdeverkossa, voidaan samalla sovelluksella kuin pass-the hash hyökkäyksessä, tallentaa Kerberokseen liittyvät tiketit. Tallennetut tiketit voi sitten ottaa käyttöön omalla tietokoneellaan ja sitten ottaa yhteyden kohteen järjestelmiin ja palveluihin tavanomaisten Windows-sovellusten kautta. Kuvassa 27 on esimerkki Kerberos tikettien selvittämisestä ja tallentamisesta. (McClure ym. 2012, 176 — 177.)



Kuva 257: WCE:n käyttö Kerberos tikettien selvittämiseksi ja tallentamiseksi (McClure ym. 2012.)

Nykyään on saatavilla sovelluksia (esim. Metasploit), joiden kirjastoissa on mittava valikoima erilaisia hyväksikäyttökeinoja valmiina käyttöön. Testaajan ei kuitenkaan tarvitse tyytyä vain painamaan nappia ja toivomaan parasta, sillä hyväksikäyttökeinoja saa muokattua sopimaan kuhunkin tilanteeseen. On mahdollista myös ottaa käyttöön mm. IDS:n väistötekniikoita. Tämän tyyliset sovellukset eivät kuitenkaan poista tarvetta perusteelliselle tiedon hankinnalle kohteesta, mutta sitä voi helpottaa. Metasploit sovellukseen voi luoda tietokannan tiedonkeräyksen tuloksia varten ja monia suosittuja työkaluja, kuten esimerkiksi nmap:a voi suorittaa suoraan Metasploitin sisältä, jolloin tulokset siirtyvät suoraan tietokantaan. (McClure ym. 2012, 79 — 81 & 170 — 172.)

Monet loppukäyttäjän käyttämät sovellukset altistavat kohteen hyökkäyksille, sillä monet niistä avaavat portin Internetiin, jotkut jopa käyttäjien tietämättä. Haavoittuvuustietokannat tarjoavat näiden keinoja näiden sovellusten hyväksikäyttöön kohdeverkkoon murtautumisessa. Kuten palveluiden hyväksikäytössä edellä, myös loppukäyttäjän sovellusten hyväksikäyttöön voi käyttää Metasploit:a. Kuvassa 28 on esitetty 50 käytetyimmän sovelluksen haavoittuvuuksien määrä vuonna 2012. (McClure ym. 2012, 181.)



Kuva 268: 50 käytetyimmän sovelluksen haavoittuvuudet 2012 (Secunia ApS 2013.)

Laiteajurit ovat myös hyväksikäytettävissä järjestelmään tunkeutuessa ja niiden hyväksikäyttö ei aina välttämättä vaadi lainkaan fyysistä kosketusta kohdejärjestelmään. Pahimmassa tapauksessa edes pääsyä kohteen tiloihin ei vaadita. Laiteajurien hyväksikäyttö muodostui keinoksi kun Johnny Cache, HD Moore ja skape huomasivat, että Windowssin WLAN-ajureita pystyi hyväksikäyttämään, kun jokin kohteen laitteista oli hyökkääjän konfiguroiman AP:n kantaman sisällä. Hyökkääjän AP lähettää erilaisia paketteja, jotka sitten tavalla tai toisella hyväksikäyttävät kohteen WLAN-ajureita. (McClure ym. 2012, 183 — 184.)

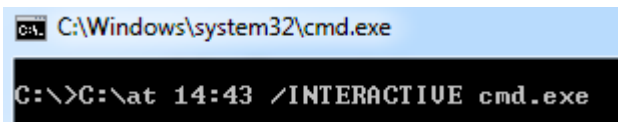
3.3.2 Todennetut hyökkäykset

Kun järjestelmään on pääsy joillakin tunnuksilla, täytyy testaajaan laajentaa oikeuksiaan. Tämä tarkoittaa käytännössä Administrator- tai SYSTEM-tason oikeuksia. Yksi tehokkaimpia keinoja tähän tarkoitukseen on erilaiset DLL-injektointi hyökkäykset. Näissä hyökkäyksissä Windowsin prosesseihin syötetään oma koodi ajettavaksi, joka sitten antaa tavoitellut oikeudet. Windows-järjestelmissä tämänkaltaista oikeuksien lisäämistä kuitenkin haittaa se että ne vaativat vuorovaikutteisen kirjautumisen toimiakseen. Suurin osa käyttäjistä ei todennäköisesti pysty suorittamaan interaktiivista kirjau-

tumista palvelimille, mutta tämä ei haittaa testaajaa, jos aiemmin haltuun saadut käyttäjätunnukset kuuluvat joihinkin monista Windows käyttöjärjestelmän ”operaattori”-ryhmistä. Kuvassa 29 on esitettynä interaktiivinen kirjautuminen. (McClure ym. 2012, 185; Microsoft 2013; Lowe, S. 2008.)

Kuva 29: Windows-käyttöjärjestelmän interaktiivinen kirjautuminen (Samuel, J. 2012)

Pääkäyttäjätaso eivät kuitenkaan ole se ylin oikeuksien taso joka voidaan saavuttaa, niiden yläpuolella on kuitenkin vielä SYSTEM tason oikeudet. Saavutettuaan pääkäyttäjän oikeudet SYSTEM oikeuksien saavuttaminen tapahtuu käyttämällä komentokehotetta ja Windows käyttöjärjestelmän Scheduler palvelua kuvan 30 osoittamalla tavalla. (McClure ym. 2012, 185; Lowe, S. 2008; Microsoft 2008.)

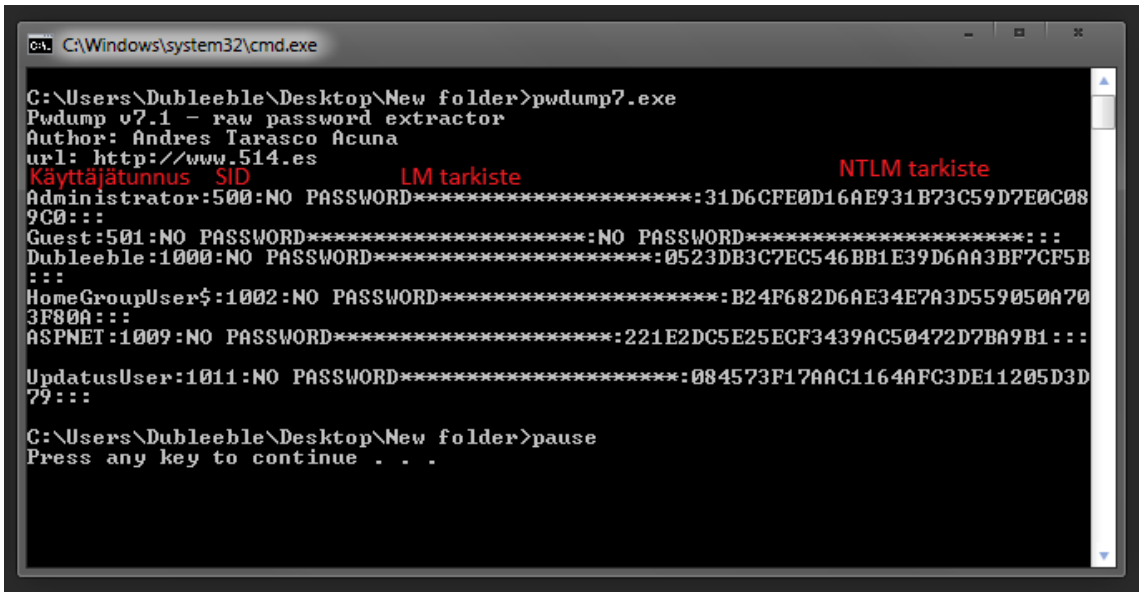


Kuva 30: Windows Scheduler palvelun käyttö SYSTEM tason oikeuksien saavuttamiseksi

Pääkäyttäjän tunnukset saatuaan testaajan seuraava kohde on salasanojen tarkisteet, jotka sijaitsevat paikallisten tunnusten osalta SAM tiedostossa (Security Accounts Mana-

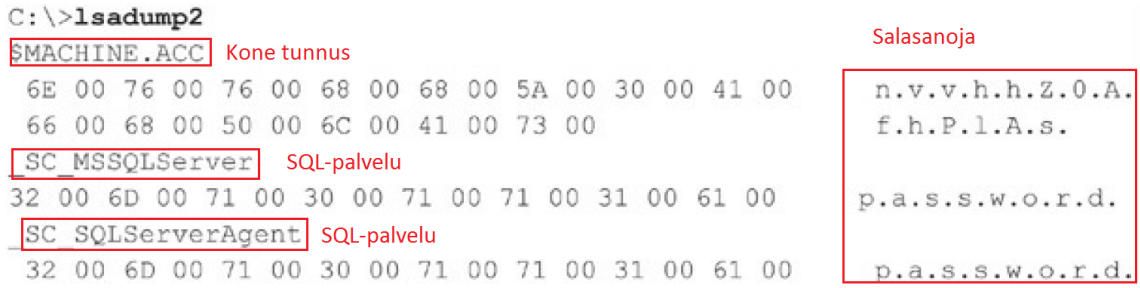
ger) tai Domain Controllerilla toimialueen tunnusten osalta. Vaikka testaaja saisi käsiinsä vain SAM tiedoston sisältämät paikalliset tunnukset, on silti mahdollista löytää tunnuksia joilla on pääsy esimerkiksi Domain Controllerille. Tämä johtuu monesti siitä että kaikille pääkäyttäjätunnuksille annetaan sama salasana. Testaajan ei siis kannata sivuuttaa paikallisia tunnuksia. (McClure ym. 2012, 187.)

Salasanojen tarkisteiden hankkimiseen on useita keinoja. Eräs keino on käyttää pdwdump sovellusta, jonka avulla kuvassa 31 on hankittu NTLM tarkisteet. (McClure ym. 2012, 187; Dagenais, T. 2013.)



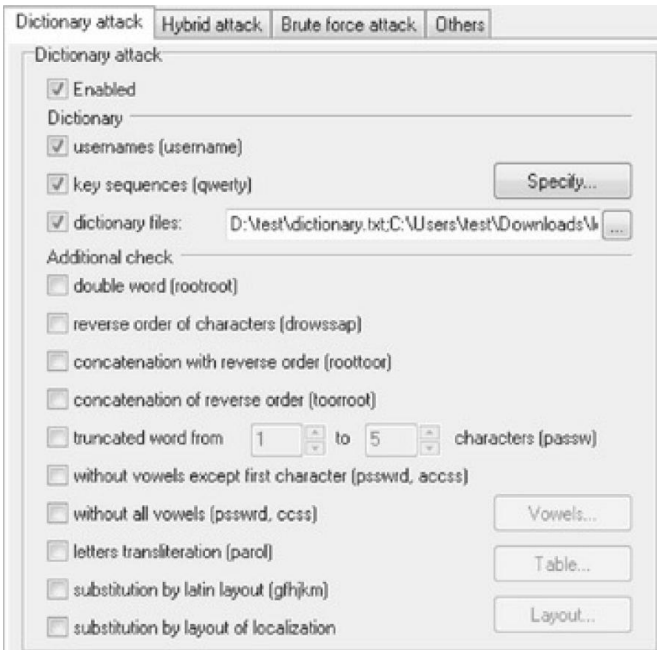
Kuva 31: pwdump sovelluksella selvitetyt tarkisteet (McClure ym.2012, 187; Dagenais, T. 2013.)

Salasanoja saa selville SAM tiedoston ja DC:in lisäksi myös esimerkiksi Windowsin rekisteristä, jossa LSA (Local Security Authority) sisältää useita eri salasanoja. Näistä esimerkkinä mainittakoon kymmenen tietokoneelle viimeksi kirjautuneen käyttäjän salasanan tarkiste ja palvelutunnusten (service account) salasanoja selkokielisinä, jotka voivat altistaa hyväksikäytölle myös muita toimialueita. Kuvassa 32 on käytetty lsadump2 sovellusta selvittämään salasanoja. . (McClure ym. 2012, 195 — 196; Damele, B. 2011.)



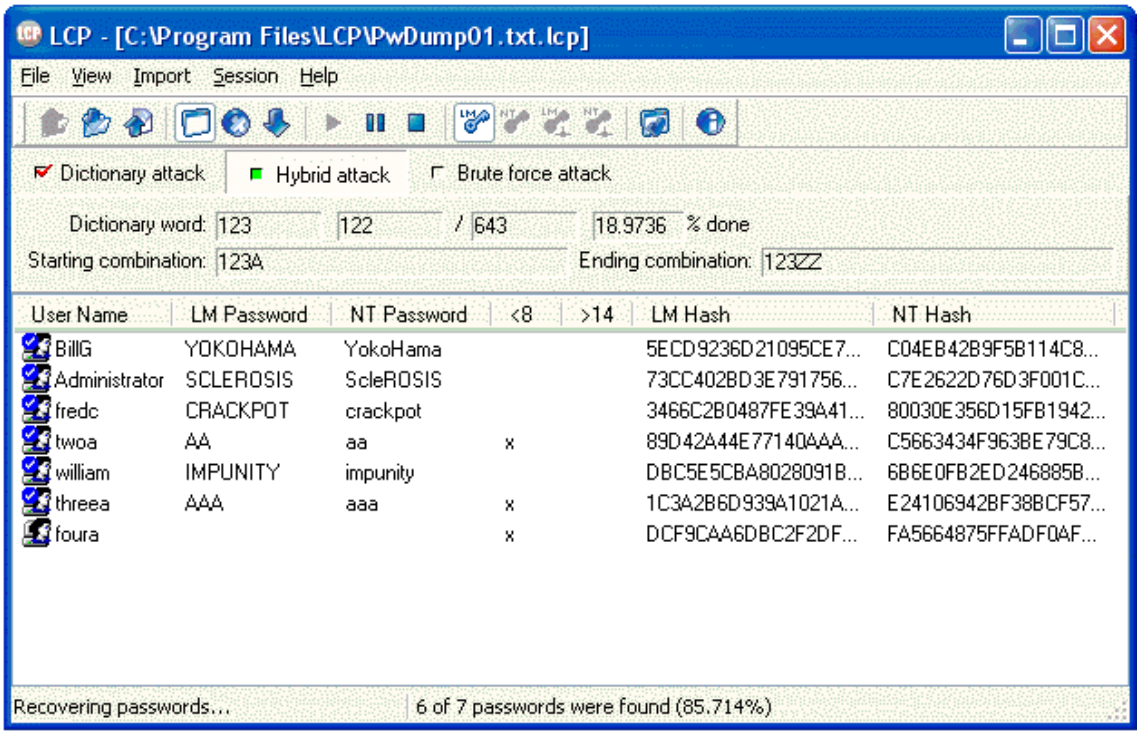
Kuva 32: lsadump2 sovelluksen LSA:sta selvittämiä selkokielisiä salasanoja (McClure ym.2012, 196.)

Tarkisteita olisi mahdollista käyttää sellaisenaan, kuten kappaleessa 3.2.1 esitetiin, mutta mm. testauksen tulosten kannalta on tärkeää selvittää salasanat tarkisteista. Salasanojen murtamiseen on tyylejä. Sanastohyökkäys perustuu nimensä mukaisesti sanastoon, jossa on erilaisia salasana vaihtoehtoja, joita sitten verrataan tarkisteisiin. Aikaisemminkin mainitussa brute force-menetelmässä tarkisteita verrataan satunnaisia merkkijonoja kunnes salasana selviää. Kummassakin keinossa on heikkoutensa: sanasto ei välttämättä ole tarpeeksi kattava ja brute-force menetelmä liiankin kattava, vaikka sen käyttämää merkistöä pystyy rajoittamaan. Useat sovellukset tarjoavatkin keinoja rajoittaa tai hienosäätää salasanamurtamista. Kuvassa 33 on esitettynä LCP sovelluksen sanastohyökkäyksen hienosäätö mahdollisuuksia. (McClure ym. 2012, 191.)



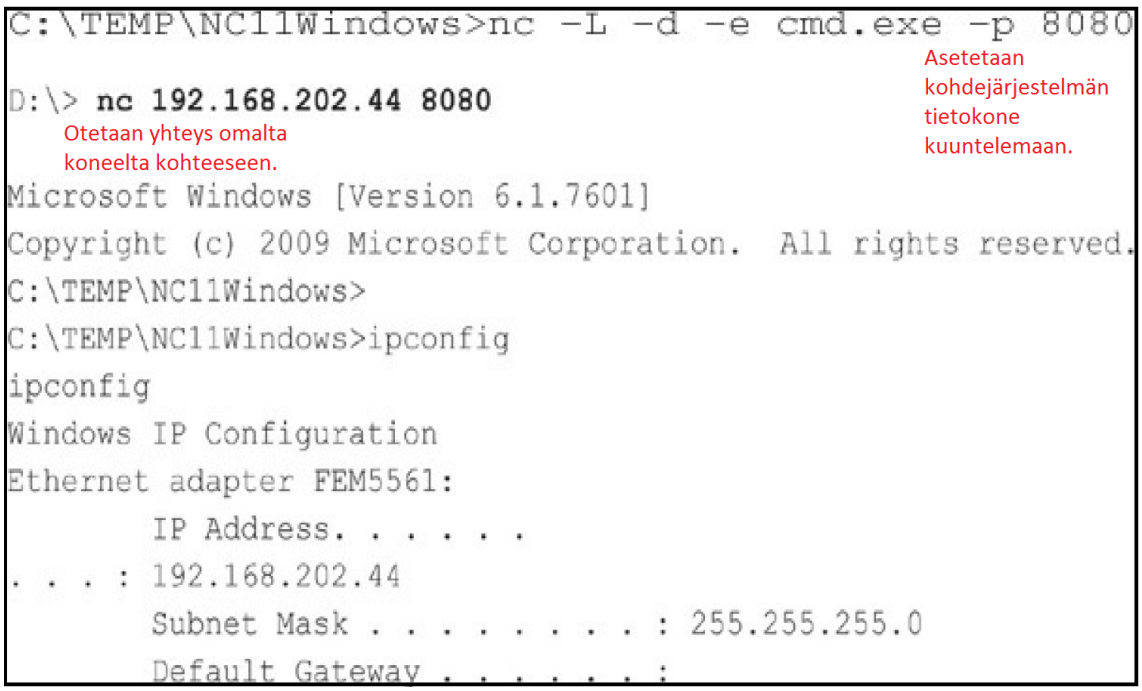
Kuva 273: LCP sovelluksen sanasto hyökkäyksen hienosäätö mahdollisuudet (McClure ym.2012, 191.)

Kuvassa 34 on puolestaan LCP:n suorittaman sanastohyökkäyksen tulokset, jotka hyvin samankaltaiset kuin pwdump:n tulokset (Kuva 32), joskaan niissä ei näy SID-numeroa.



Kuva 34: LCP:n sanastohyökkäyksen tulokset (LCPSoft 2013.)

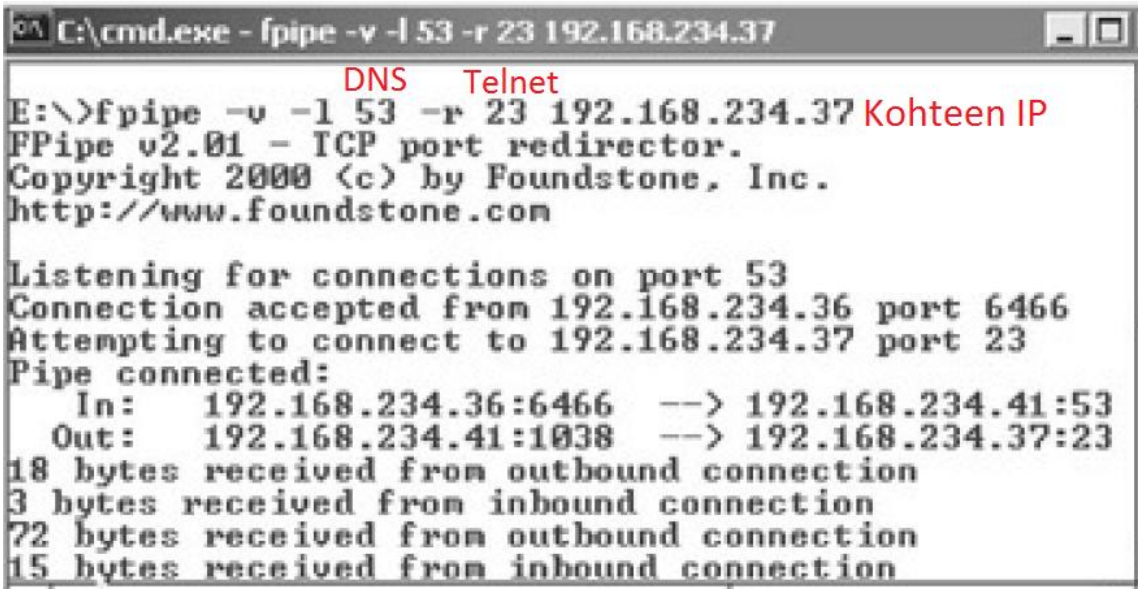
Testauksen määrittelystä riippuen voi olla tarpeen pystyä hallitsemaan kohdejärjestelmää myös etähallinnan kautta, jonka tarkoituksena on vahvistaa testaajan hallintaa kohdejärjestelmästä. Testaajan käyttöön löytyy keinoja, jotka toimivat kokonaan komentokehotteesta tai sellaisia, joissa tarvitaan sekä komentokehotetta että graafista käyttöliittymää. Puhtaasti komentokehotteessa pyörivästä etähallinta keinosta on esimerkki kuvassa 35, jossa netcat asetetaan kuuntelemaan tiettyyn porttiin ja käynnistämään tietty sovellus, kun määriteltyyn porttiin otetaan yhteys. Komentokehote C (C:\) on kohdejärjestelmän tietokone ja komentokehote D(D:\) testaajan tietokone. (McClure ym. 2012, 200 — 201; Keohan, J. 2010.)



Kuva 3528: Kohteen ottaminen etähallintaan netcat:n avulla (McClure ym.2012, 200 — 201.)

Graafinen etähallinta, olettaen että Microsoftin TS ei ole käytössä kohteessa, vaatii sopivan etähallinta sovelluksen asentamista kohteeseen. RealVNC:n VNC:tä (Virtual Network Computing) on yksi monista. Valittu sovellus (VNC) asennetaan kohteeseen, jonka lisäksi se vaati muutaman rekisteri muutoksen kohteeseen. (McClure ym. 2012, 202 — 204.)

Porttien uudelleenohjaus toimii etähallinta keinona sellaisissa tilanteissa, joissa palomuuri estää muihin etähallinta keinoihin liittyvän liikenteen. Porttien uudelleenohjauksessa asetetaan kohde kuuntelemaan sellaista porttia, johon halutaan saada yhteys, esimerkiksi netcat:lla (kuva 35). Varsinainen portin uudelleenohjaus asetetaan omalla tietokoneella, esimerkiksi fpipe:n avulla. Kuvassa 36 fpipe on asetettu kuuntelemaan paikallista porttia 53 (DNS) ja ohjaamaan se kohteen porttiin 23 (Telnet). (McClure ym. 2012, 204 — 206; McAfee 2013; Gimer, J. 2009; Klevinsky ym. 2002, 302 — 303.)



Kuva 36: Fpipen käyttö porttien uudelleenohjauksessa (McClure ym.2012, 206.)

Testaaja voi nyt ottaa yhteyden paikallisesti, eli fpipe sovellukseen, porttiin 53 Telnet sovelluksellaan muodostaakseen yhteyden kohteeseen, sillä fpipe ottaa yhteyden netcat sovellukseen, joka kuuntelee porttia 23 ja ohjaa liikenteen todelliseen kohteeseensa. Myös paluu liikenne ohjautuu käyttäen porttia 53. Portin uudelleen ohjauksen voi toteuttaa muillakin porteilla jotka ovat kohteessa auki. (McClure ym. 2012, 204 — 206; McAfee 2013; Gimer, J. 2009; Klevinsky ym. 2002, 302 — 303.)

3.4 Raportointi

Lopuksi kun kaikki sopimuksessa määritellyt toimet on suoritettu, pitää testauksen tulokset esittää asiakkaalle. Raportin kirjoittamisessa pitää ottaa huomioon liikkeenjohdolliset sekä tekniset asiat. Löydökset tulee esittää mahdollisimman yksityiskohtaisesti, kuvaajien ja lukujen avulla yms. tiedon avulla mitä testauksen aikana on saatu selville. Näin saadaan aikaan kunnollinen kuvaus kohdejärjestelmän haavoittuvuuksista ja niiden vaikutuksesta asiakkaan liiketoimintaan. Raportti usein sisältää asiakasyrityksen johdolle suunnatun tiivistelmän, jossa kuvaillaan miten testaus suoritettiin, testauksen tulokset sekä yleisen tason suositukset tulosten perusteella. Tulosten perusteella tehdään myös arvio siitä mitä suositusten toteuttaminen maksaisi. (Saindane 2013, 9; The Sans Institute 2010.)

Testauksen aikana löydetyistä haavoittuvuuksista kuvataan sen lähde ja syy kyseiselle haavoittuvuudelle, haavoittuvuuden vaikutus, kuinka todennäköistä on että kyseistä

haavoittuvuutta käytetään hyväksi, millaisen riskin haavoittuvuus aiheuttaa ja suositus ongelman korjaamiseksi. Näiden kuvausten tukena tulee olla kuvankaappauksia, keino miten haavoittuvuutta käytettiin hyväksi (ohjelma tms.) tai muuta soveltuvaa tietoa. (Saindane 2013, 9; The Sans Institute 2010.)

Raportin rakenne voisi esimerkiksi olla:

1. Kansilehti
2. Raportin tiedot
3. Versio
4. Sisällys
    a. Liikkeenjohdolle suunnattu tiivistelmä
        i. Työn laajuus
        ii. Projektin tavoitteet
        iii. Tehdyt oletukset
        iv. Aikajana
        v. Tulosten tiivistelmä
        vi. Suositusten tiivistelmä
    b. Menetelmät
    c. Tulokset
        i. Haavoittuvuudet
    d. Yhteenveto
5. Kuvaluettelo
6. Lähteet
7. Liitteet
8. Sanasto

(Saindane 2013, 9; The Sans Institute 2010.)

4 WPK-VERKON HAAVOITTUVUUSANALYYSI

Tässä testauksessa kartoitettiin haavoittuvuuksia TAMK:n verkossa sijaitsevasta WPK-verkosta. Täysimittaisesta tunkeutumistestauksesta ei siis ole kyse, mutta monia sen tekniikoita käytettiin. Testauksen lähtökohtana oli että testaus suoritetaan verkon sisältä ja samaa IP-osoitetta on mahdollista käyttää läpi testauksen. Testauksessa ei tarvinnut huolehtia havaituksi tulemisesta, sillä siitä oli sovittu etukäteen. Testaus suoritettiin aikana jona kohdeverkon käyttöaste oli pieni. Testilaitteistona toimi kannettava tietokone johon oli asennettu Backtrack Linux 5 r3. Muita laitteita ei tarvittu.

4.1 Suunnittelu

Suunnitelma koostui testaustilanteen kuvailusta, testattavista asioista, WLAN testauksesta, lähiverkon uhista, pakettikaappauksesta sekä mies välissä hyökkäyksestä. Testattavat asiat muodostivat suunnitelman ytimen, johon kuului järjestelmän jalanjälkien tutkimista, skannaamista sekä haavoittuvuuksien analysointia. Suunnitelma perustui sen hetkiseen tietoihin aiheesta sekä osittain Backtrack Linuxin tarjoamiin mahdollisuuksiin.

4.2 Tietojenkeräys

Testaus aloitettiin selvittämällä kohteen DNS-tietoja dnsrecon nimisellä python skriptillä:

./dnsrecon.py -d wpk.tpu.fi

Valitsimella ”d” ja sen jälkeisellä osoitteella määriteltiin kohde toimialue. (Aldeid 2012.) Dnsrecon skriptin tulokset (Liite 1) kertoivat odotetusti kohteen nimipalvelimet, mutta niiden lisäksi tulosten perusteella voitiin päätellä seuraavia asioita:

- DNS:n SOA tietueen sijainti
- Sähköpostipalvelin
- Kohteessa käytetään Kerberos todentamista
- Kohteessa on käytössä Active Directory

DNS tietoja yritettiin hankkia myös fierce nimisellä skriptillä. Valitsimella ”wide” Fierce skannasi koko aliverkon (ha.ckers 2013.):

./fierce.pl -dns wpk.tpu.fi -wide

Fierce DNS tietojen hankkimisen lisäksi yritti vyöhykesiirtoa DNS-palvelimia vastaan siinä kuitenkaan onnistumatta. Sen kuitenkin onnistui selvittää joitakin IP-osoitteita ja niitä vastaavia nimiä, joita dnsrecon ei saanut selville (Liite 2).

Pelkillä IP-osoitteilla ja niitä vastaavilla nimillä ei tee mitään, jos laitteet, joita ne edustavat eivät ole päällä. Kohteiden tilan selvittämiseksi suoritettiin selvinneitä IP-osoitteita vastaan ARP-skannaus, joka toteutettiin nmap nimisellä sovelluksella:

sudo nmap -sn –PR [Kohde IP][aliverkkomaski}

Valitsimella “sn” määriteltiin, että tämän skannauksen yhteydessä ei suoriteta porttiskannausta ja valitsimella ”PR” otettiin käyttöön ARP ping. (Nmap.org 2013.) Skannaus paljasti yhteensä 40 laitteeen olevan päällä. Lisäksi skannaus paljasti sellaisten laitteiden IP-osoitteen, jotka eivät DNS tietoja etsiessä paljastuisi. Näihin laitteisiin sisältyi Ciscon, Broadcom:n ja Buffalon laitteita, kun katsoo millaisia laitteita nämä yrityksen valmistavat selviää niiden rooli verkossa. Ciscon laite on todennäköisesti reititin tai kytkin, Broadcomin laite AP (Access Point). ja Buffalon laite levypalvelin. Alta löytyy kaksi esimerkkiä ARP-skannauksesta, joista ensimmäisessä on löydetty Buffalon laite. Toisessa esimerkissä on löydetty Broadcomin laite.

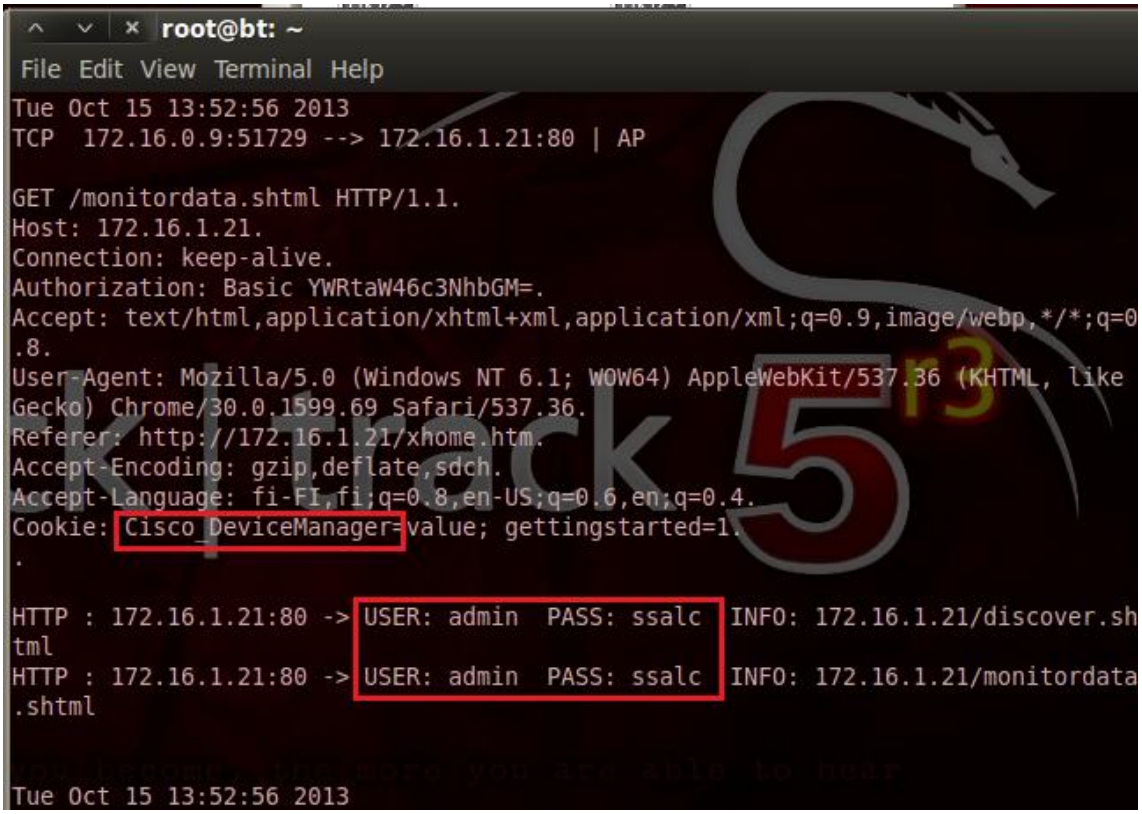
Nmap scan report for kellari.wpk.tpu.fi (172.16.1.60)
Host is up (0.000099s latency).
MAC Address: 00:16:01:7E:A1:F0 (Buffalo)

Nmap scan report for 172.16.0.10
Host is up (0.00022s latency).
MAC Address: 00:10:18:30:DE:7A (Broadcom)

Porttiskannauksella, perustuen edellisiin tuloksiin, selvitettiin mitä portteja oli avoinna selvinneissä kohteissa.

sudo nmap -Pn [Kohde IP]

Huolestuttavain tulos oli että kuinka monessa kohteessa oli auki jonkin palvelun tietoturvallinen versio sekä tavallinen, tietoturvattomampi versio. Esimerkiksi monesta kohteesta löytyi sekä avoin HTTPS (Hyper Text Transfer Protocol Secure) ja http (Hyper Text Transfer Protocol). Monen kohteen WWW-selaimessa toimivaan hallintapaneeliin oli näin helppo saada yhteys tai esimerkiksi käynnistää mies välissä hyökkäys tällaista kohdetta vastaan salasanan selvittämiseksi. Kuvassa 37 näkyy kuinka mies välissä hyökkäyksellä on asetuttu Ciscon laitteen ja työaseman, joka ottaa yhteyden laitteen hallintapaneeliin http:n yli, väliin.



Kuva 297: Mies välissä hyökkäys Ciscon laitteen ja työaseman välillä

Kuten kuvasta 37 voi huomata, http yhteys paljastaa käytetyt kirjautumistiedot suhteellisen helposti ja luettavassa muodossa. Sama, tietoturvallinen-tietoturvaton kuvio, toistui monessa kohteessa Telnetin ja SSH:n (Secure Shell) kohdalla. Näiden palveluiden

kohdalla kannattaisi sammuttaa turvattomampi vaihto ja siirtyä käyttämään vain turvallisempaa vaihtoehtoa.

Porttiskannaus myös monilta osin vahvisti aikaisempia tuloksia sekä kertoi enemmän monesta kohteesta. Selvisi missä kohteissa ja missä porteissa pyöritetään Microsoftin AD:ta. Tietyiltä osin tulokset esittivät eriskummallisia tuloksia, mutta pienen tutkimuksen jälkeen näillekin porteille löytyi todennäköisempi vaihtoehto. Ensimmäisenä esimerkkinä on porttiskannaus samasta laitteesta, josta on esimerkki ARP-skannauksissa. Esimerkistä on korostettu http ja https aikaisemmin todetun perusteella.

```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-10-15 14:36 EEST
Nmap scan report for kellari.wpk.tpu.fi (172.16.1.60)
Host is up (0.00057s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
873/tcp   open  rsync
8873/tcp  open  dxspider
22939/tcp open  unknown
MAC Address: 00:16:01:7E:A1:F0 (Buffalo)
```

Toisena esimerkkinä on kuva 37 esittämän mies välissä hyökkäyksen kohteen porttiskannaus tulokset.

```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-10-15 13:48 EEST
Nmap scan report for ahk.wpk.tpu.fi (172.16.1.21)
Host is up (0.0060s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:23:EA:BE:A6:C1 (Cisco Systems)
```

Käyttöjärjestelmän tunnistaminen on olennaista kun etsitään järjestelmän haavoittuvuuksia. Nmap:n valitsimella ”O” selvitettiin kohde IP-osoitteesta käyttöjärjestelmä (Nmap.org 2013.)

sudo nmap -O [Kohde IP]

Pääosin tulokset olivat luotettavia ja sellaisia joita aikaisempien tulosten avulla saattoikin odottaa. Skannaus tunnisti käyttöjärjestelmiä Ciscon laitteista, Linux järjestelmistä sekä Windowseja niissä kohteissa missä saattoi olettaakin olevan Windows käyttöjärjestelmänä. Alta löytyy muutamia esimerkkejä tuloksista. Ensimmäisessä esimerkissä skannaus on tunnistanut Ciscon laitteen käyttöjärjestelmän.

Device type: switch
Running: **Cisco IOS 12.X**
OS CPE: cpe:/h:cisco:catalyst_2960 cpe:/h:cisco:catalyst_3560 cpe:/o:**cisco:ios:12.2**
OS details: **Cisco Catalyst 2960 or 3560 switch (IOS 12.2)**
Network Distance: 2 hops

Device type: general purpose
Running: **Microsoft Windows 7|2008**
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: **Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8**
Network Distance: 2 hops

Pelkkien palveluiden, porttien ja käyttöjärjestelmien avulla löytäisi varmasti haavoittuvuuksia, mutta sitä voisi verrata hakuammuntaan, joten tarkkojen sovellus versioiden selvittäminen on oleellista. Tämä suoritettiin nmap:lla ja sille määriteltiin valitsimet ”sV”, joka määrittelee että kyseessä on palveluiden versio skannaus, ja ”p”, jonka lisäksi määriteltiin portit, jotka skannataan. (Nmap.org 2013.) Määritelty portti väli perustui aikaisempien tulosten avoimiin portteihin.

nmap -sV [Kohde IP] -p 22-8873

Tulokset olivat vaihtelevia, mutta kuitenkin käyttökelpoisia. Joistakin palveluista selvisi vain tarkempi nimi, mutta versionumeroa. Toisaalta joistakin palveluista tuli hyvinkin tarkkoja versiotietoja. Myös tyhjiä tuloksia oli jonkin verran. Alla on esitettynä esimerkkejä versioskannauksen tuloksista. Ensimmäisessä esimerkissä on skannattu edellä esitetyn mies välissä hyökkäyksen kohteen palveluiden versiot.

Nmap scan report for kellari.wpk.tpu.fi (172.16.1.60)
Host is up (0.0011s latency).
Not shown: 8846 closed ports
PORT STATE SERVICE VERSION
80/tcp open http **Apache httpd 1.3.34** ((Unix) mod_ssl/2.8.25 **OpenSSL/0.9.7e**)

139/tcp open netbios-ssn **Samba smbd 3.X (workgroup: WPK**)
443/tcp open ssl/http Apache httpd 1.3.34 ((Unix) mod_ssl/2.8.25 OpenSSL/0.9.7e)

445/tcp open netbios-ssn **Samba smbd 3.X (workgroup: WPK)**
873/tcp open rsync (protocol version 29)
8873/tcp open ssl/rsync (protocol version 29)

Starting Nmap 6.25 (http://nmap.org) at 2013-10-18 10:18 EEST
Nmap scan report for 172.16.1.1
Host is up (0.021s latency).
Not shown: 8849 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh **Cisco SSH 1.25 (protocol 2.0)**
23/tcp open telnet Cisco router telnetd
4786/tcp open unknown
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

4.3 Lähiverkon uhat

Osana testausta suoritettiin myös erilaisia hyökkäyksiä ja tutkittiin miten kohdeverkko reagoi tai saako siitä tietoja irti.

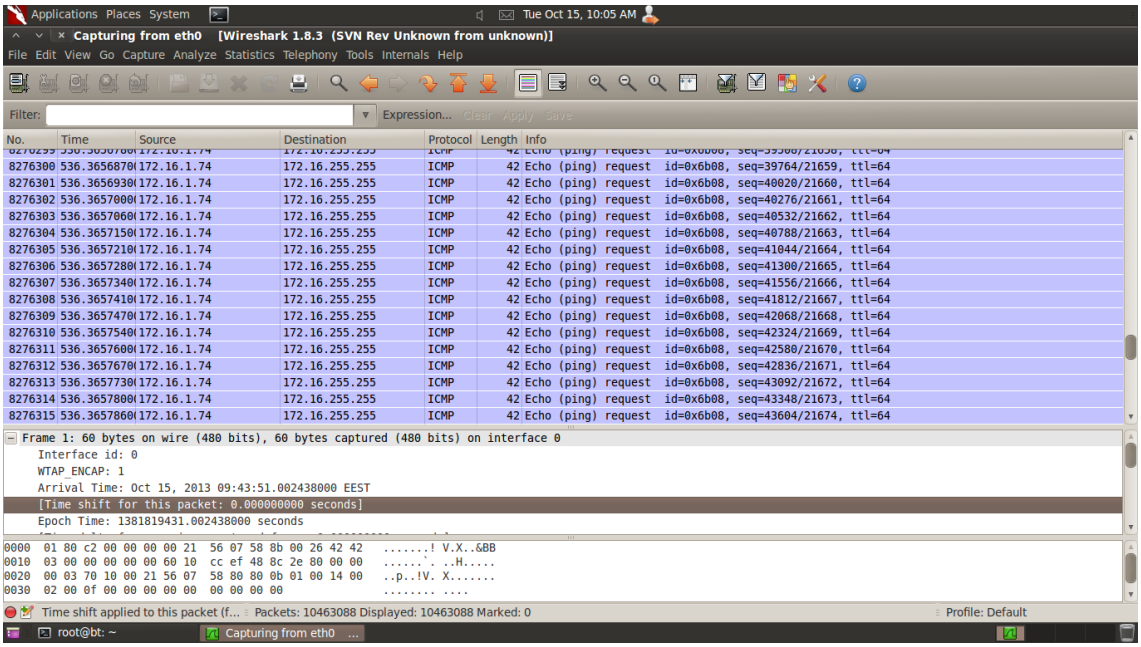
4.3.1 SMURF hyökkäys

Smurf hyökkäyksessä kohdeverkkoon lähetetään jatkuvasti ICMP-paketteja, joiden lähettäjäksi on väärennetty halutun kohteen IP-osoite. Pakettien kohteena on broadcast-osoite. Broadcast-osoitteen edustaessa verkon kaikkia osoitteita seurauksena on että kaikki vastaavat paketteihin. Seurauksena on kohteen hukkuminen ICMP-paketteihin, tästä seuraa kohteen muuttuminen käytännössä käyttökelvottomaksi. (Rouse, M. 2007.) Käytin Smurf hyökkäykseen hping3 sovellusta. Hyökkäyksen kohteena toimi yksi WPK-verkon DNS-palvelimista.

hping3 -1 –flood –a [Kohde IP][Broadcast osoite*]*

Valitsin “1” asetti hping3:sen käyttämään ICMP:tä, ”flood” mahdollisti pakettien lähettämisen mahdollisimman nopeasti ja ”a”:lla määriteltiin että pakettien lähettäjäksi väärennetään haluttu kohde. (0Day Security 2010.)

Hyökkäyksen vaikutukset olivat huomattavissa lähes välittömästi. Kohteeseen yhteydessä ollut wpk-verkon harjoittelija huomasi käytön alkavan hidastumaan, kunnes jonkin ajan kuluttua katkesi. Verkon laajuiset vaikutukset oli todettavissa kun muihin palvelimiin yhteyden muodostaminen epäonnistui. Myös Internet yhteys oli hyökkäyksen aikana käyttökelvoton. Kuvassa 38 on hyökkäyksen aikana tehty pakettikaappaus.



Kuva 3830: Pakettienkaappaus Smurf hyökkäyksen aikana

Yksi keino Smurf hyökkäyksien estämiseksi olisi estää IP directed broadcast niissä reitittimien porteissa jotka eivät tarvitse sitä. On mahdollisuus myös käyttää pääsylistoja reitittimillä estämään hyökkäykseen liittyvää liikennettä. Pääsylistojen haittana tässä yhteydessä on kuitenkin että ne samalla estävät TCP/IP-protokollaan perustuvien diagnostiikka sovellusten käytön. (Dargin, M. 2002; Martin, M. 2002.)

4.3.2 SYN flood hyökkäys

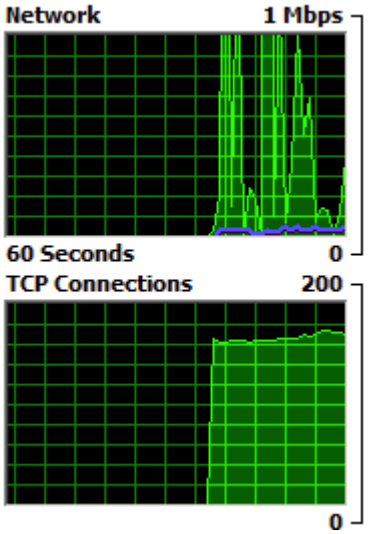
SYN flood hyökkäyksessä haluttuun kohteeseen lähetetään TCP-yhteyspyyntöjä nopammin kuin niitä pystytään käsittelemään. Jokaisessa lähetetyssä paketissa on SYN

lippu asetettu ja jokainen paketti näyttää tulevan eri lähteestä. Kohteen yhteysjono täyttyy, jonka jälkeen uudet yhteyspyynnöt hylätään. (Internet Security Systems 2013.)

SYN flood hyökkäyksen toteutin myös käyttäen hping3 sovellusta. Kohteena oli www-palvelin, joka vastasi wpk-verkon www-sivuista.

sudo hping3 -i u1 -S -p [Kohde portti][Kohde IP]

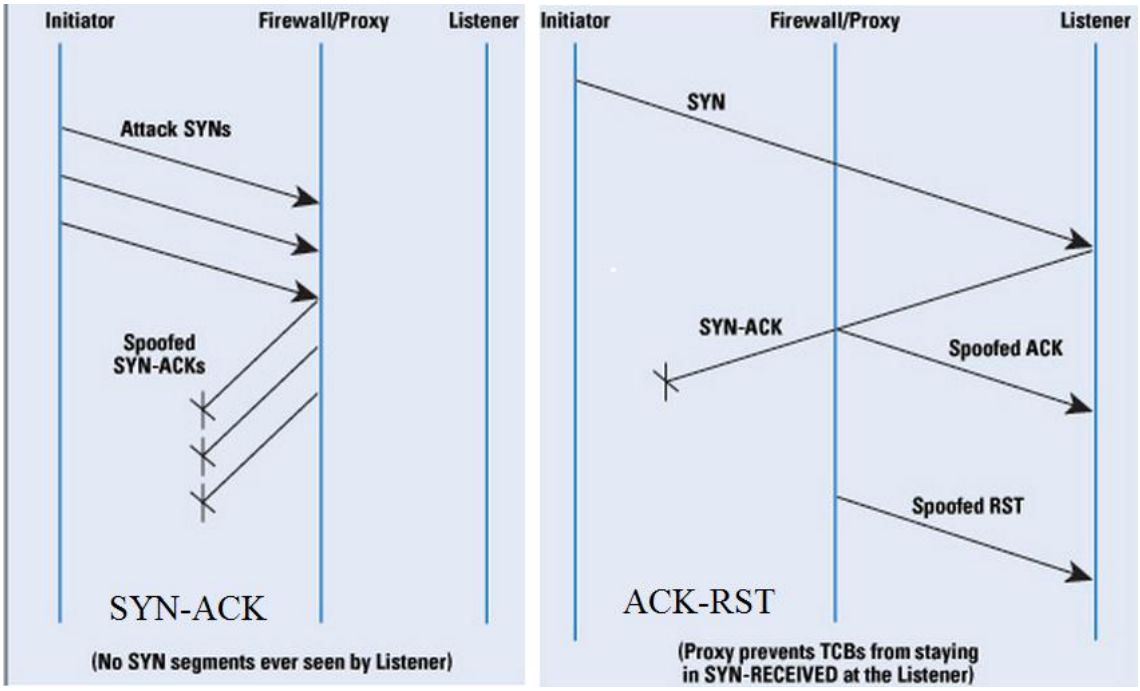
Valitsimella “i u1” pakettien lähetysväli määriteltiin yhden mikrosekunnin suuruiseksi. ”S” valitsimella määriteltiin lähetettäviin paketteihin SYN lippu päälle. Kohde portti asetettiin valitsimella ”p”. (0Day Security 2010.) Hyökkäyksen aikana wpk-verkon www-sivuja ei voinut käyttää ja kohteena olevan palvelimen käyttö oli huomattavan hidasta. Kuvasta 39 voi huomata että kohdeverkossa olevat TCP yhteydet kasvoivat huomattavasti.



Kuva 39: Kohdeverkon TCP yhteyksien määrä SYN flood hyökkäyksen aikana

SYN flood hyökkäystä vastaan voi puolustautua ottamalla käyttöön SYN välimuistin tai SYN cookiet. SYN välimuistin käyttö SYN flood hyökkäyksen torjumisessa perustuu siihen että TCP-yhteydelle ei anneta täyttä TCB:tä (Transmission Control Block) ennen kuin yhteyden muodostajan olemassaolosta voidaan varmistua. SYN cookie keinossa yhteyksiä ei, jonon täyttyessä pudoteta, vaan toiminta jatkuu ikään kuin jonoa olisi kasvatettu. Yhteyden muodostajalle lähetetään normaalisti SYN-ACK-viesti, mutta SYN tiedot poistetaan jonosta. Jos tämän jälkeen saadaan asianmukainen ACK-viesti, voidaan yhteydenmuodostus palauttaa jonoon alkuperäiselle paikalleen. Verkon laitteet,

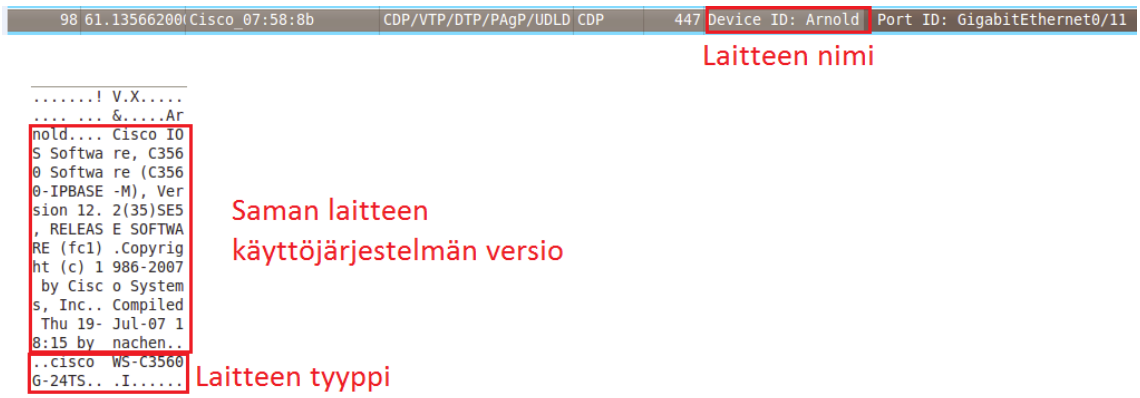
reitittimet ja palomuurit, voidaan asettaa suodattamaan liikennettä siten että SYN flood hyökkäyksen paketteja ei reititetä eteenpäin. Toinen verkon laitteisiin perustuva keino on asettaa reititin lähettämään väärennettyjä SYN-ACK lippuja sisältäviä paketteja hyökkääjän suuntaan. Toinen samankaltainen puolustautumiskeino on lähettää hyökkääjän kohteelle väärennettyjä ACK- ja RST lippuja sisältäviä paketteja. Kuvassa 40 on esitetty SYN-ACK sekä ACK-RST puolustus. (Eddy, W. 2013.)



Kuva 310: SYN-ACK puolustuksen toiminta (Eddy, W. 2013.)

4.3.3 Pakettienkaappaus

Pakettienkaappauksen suoritin Wireshark-ohjelmalla. Toiminnan luonteesta johtuen pakettien kaappauksella ei ollut varsinaista kohdetta vaan siinä kuunneltiin passiivisesti kaikkea verkon liikennettä. Pakettienkaappauksella selvisi tietoja sovellusten versioista, laitteista sekä pääsylistoista. Kuvassa 42 on otteita Wiresharkin kaappaamasta liikenteestä, josta voidaan nähdä että on kaapattu liikennettä koskien Ciscon laitetta. Tästä laitteesta on saatu selvitettyä nimi, käyttöjärjestelmän versio sekä tyyppi.

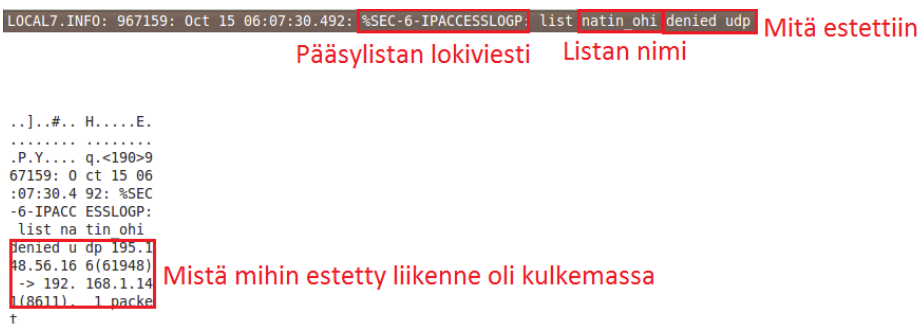


Kuva 322: Ciscon laitteesta pakettikaappauksen avulla selvinneitä tietoja

Verkon liikenteestä selvisi myös WWW-palvelimen käyttämä sovellus ja sen versio, kuten kuvasta 43 voi huomata.

Kuva 333: Pakettikaappauksella saatu tieto WWW-palvelimen sovelluksesta ja sen versiosta

Pakettikaappauksella voitiin myös havaita verkossa käytössä oleva pääsylista. Kaapatun paketin yksityiskohdat on esitetty kuvassa 44. (Cisco 2013.)



Kuva 344: Pakettikaappauksella selvinneitä pääsylista tietoja

4.3.4 Mies välissä hyökkäys

Mies välissä hyökkäys on tuloksiltaan hyvin samankaltainen kuin pakettienkaappaus, mutta on keinona aktiivinen, kun pakettienkaappaus oli passiivinen. Hyökkäyksen teoriaa esiteltiin kappaleessa 3.2.1 ja kuvassa 26. Mies välissä hyökkäys toteutettiin ettercap nimisellä sovelluksella, jonka avulla asetuin wpk-verkon harjoittelijan työaseman ja palvelimen väliin.

ettercap -T -M arp:oneway,remote /Kohde IP 1/ /Kohde IP 2/

Ettercapin määrittely erosi hieman muista käytetyistä sovelluksista. Valitsin ”T” määritteli, että käytetään komentokehote versiota ettercapista, ja ”M” että suoritetaan mies välissä hyökkäys. ”arp” määritteli hyökkäyksen toteutuskeinoksi ARP myrkytyksen, ”oneway” myrkytyksen yksisuuntaiseksi kohteesta 1 kohteeseen 2 ja ”remote” kaappaamaan sellaista liikennettä joka kulkee jommankumman kohteen läpi. (Tech Juice 2011.) Hyökkäyksen tuloksia esitettiin jo kuvassa 39, mutta lisäksi kuvassa 45 on tilanne, jossa pystyttiin lukemaan työasemalta käytettyjä www-osoitteita.

Kuva 355: Mies välissä hyökkäyksen aikana selvinneitä www-osoitteita

5 POHDINTA

Varmasti joistakin järjestelmistä voitaisiin sanoa niiden olevan tietoturvallisia, mutta se ei ole niin yksiselitteinen käsite. Aina löytyi jokin keino kiertää tietoturva tai vähintään sellaisen mahdollisuus, kuten usein huomasin tätä opinnäytetyötä kirjoittaessa. Yritysten on hyväksyttävä jokin riskitaso, joka on suhteutettu liiketoimintaansa, sillä ”murtovarman” järjestelmän toteuttaminen on kallista ja sen käyttö haittaisi liiketoimintaa.

Tunkeutumistestauksen käytänteet ovat kuin missä tahansa projektissa, se tarkasti määritelty ajallisesti ja mitä testauksen aikana tehdään, ja ei tehdä. Tunkeutumistestaus esiteltiin Windows näkökulmasta, mutta joitakin hyökkäyksiä tai muita kohtia, jotka liittyivät Windowsiin ominaisuuksiin, on siirrettävissä sellaisenaan esimerkiksi Linux kohteeseen.

Tämän työn perusteella voi miettiä onko tunkeutumistestaus se mitä tarvitsemme? Onko jotain mitä meidän asiakkaan pitäisi ottaa huomioon? Onko ulkoistamamme palvelu ottanut näitä asioita huomioon?

Työssä ei käsitelty tietoturvallisuuden perusteitta, kuten koulutusta tai tietoturvapolitiikan muodostamista. Näin jälkeenpäin ajateltuna rajaus oli oikea, sillä tunkeutumistestauksestakin olisi helposti kirjoittanut enemmän. Rajauksen puolesta puhuu sekin että tunkeutumistestausta ei kannata edes harkita jos perusasiat eivät ole kunnossa. Kypsymättömässä tietoturvaympäristössä testaajalla ei ole asiakkaalle juurikaan tarjottavaa.

Aihe oli laaja, josta olisi helposti saanut useammankin opinnäytetyön. Käsittelin omassa työssäni vain tunkeutumistestausta lähiverkkoon. Eräs hieno ja kiinnostava parin kanssa tehtävä opinnäytetyö olisi ollut, jossa toinen testaa langallista ja langatonta lähiverkkoa ja toinen kohteen fyysistä turvallisuutta.

LÄHTEET

0Day Security. 2010. Testing firewall rules with Hping3 – examples. Luettu 15.11.2013.
http://0daysecurity.com/articles/hping3_examples.html

0x0e.org | pentesting perspective. 2008. Pentesting Skillset. Luettu 6.11.2013
http://hexesec.wordpress.com/2008/07/05/pentesting-skillset/

Aldeid. 2012. Basic syntax. Luettu 15.11.2013.
http://www.aldeid.com/wiki/Dnsrecon#Basic_syntax

Amplia Security. 2012. Windows Credentials Editor (WCE) F.A.Q. Luettu 12.11.2013.
http://ampliasecurity.com/research/wcefaq.html

ARIN – American Registry for Internet Numbers. 2013. Luettu 7.9.2013.
https://www.arin.net/

Bangash Hacker. 2013. How to hack computer in LAN. Luettu 11.11.2013.
http://bangash-hacker.blogspot.fi/2011/07/how-to-hack-computer-in-lan.html#

Raj Chandel. 2013. Google Hacking with Site Digger Tool. Luettu 8.11.2013.
http://www.hackingarticles.in/google-hacking-with-site-digger-tool/

Cisco. 2010. Cisco Model DPC3825 and EPC3825 8x4 DOCSIS 3.0 Wireless Residential Gateway Use Guide. Luettu 9.7.2013.
http://www.cisco.com/web/consumer/support/userguides2/4021196_B.pdf

Cisco. 2013. Understanding Access Control List Logging. Luettu 15.11.2013.
http://www.cisco.com/web/about/security/intelligence/acl-logging.html

Corelan Team. 2008. Securing Windows Server 2008 and Active Directory. Luettu 25.10.2013.https://www.corelan.be/index.php/2008/04/18/securing-windows-server-2008-and-active-directory/

Thomas Dagenais. 2013. Cracking Windows NTML Passwords with GPU. Luettu 3.12.2013.
http://howtheyhack.com/cracking-windows-ntml-encrypted-passwords/

Bernardo Damele. 2011. Dump Windows password hashes efficiently - Part 3. Luettu 13.11.2013.
http://bernardodamele.blogspot.fi/2011/12/dump-windows-password-hashes_20.html

Mark Dargin. 2002. How to prevent a Smurf attack. Luettu 15.11.2013.
http://searchenterprisedesktop.techtarget.com/tip/How-to-prevent-a-Smurf-attack

DragonJAR. 2009. Grendel-Scan. Luettu 10.11.2013.
http://www.dragonjar.org/grendel-scan.xhtml

DragonJAR. 2008. Laboratorios: Hacking – Técnicas y contramedidas – Enumeración del objetivo I. Luettu 11.11.2013.
http://labs.dragonjar.org/laboratorios-hacking-tecnicas-y-contramedidas-enumeracion-del-objetivo-i

Patrick Dunstan. 2011. Attacking LM/NTLMv1 Challenge/Response Authentication. Luettu 12.11.2013.
http://www.defenceindepth.net/2011/04/attacking-lmntlmv1-challengeresponse_21.html

EC-Council. 2013. Certified Ethical Hacker. Luettu 6.11.2013.
http://www.eccouncil.org/Certification/certified-ethical-hacker

EC-Council. 2013. Licensed Penetration Tester. Luettu 6.11.2013.
http://www.eccouncil.org/Certification/licensed-penetration-tester

Wesley M. Eddy. 2013. Defenses Against TCP SYN Flooding Attacks. Luettu 15.11.2013.
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-4/syn_flooding_attacks.html

Federal Office for Information Security. 2003. Study – A Penetrration Testing Model. Luettu 5.11.2013
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile

Nicolas Gerard. 2009. LDAP – LDP Client. Luettu 11.11.2013.
http://gerardnico.com/wiki/windows/ldp

GIAC. 2013. Global Information Assurance Certification. Luettu 6.11.2013.
http://www.giac.org/

Joshua Gimer. 2009. TOTW: Port Redirection (nc, socat, ssh, fpipe, cryptcat). Luettu 14.11.2013.
http://itsecops.blogspot.fi/2009/08/totw-port-redirection-nc-socat-ssh.html

Ha.ckers. 2013. Fierce Domain Scan. Luettu 15.11.2013.
http://ha.ckers.org/fierce/

Hackers For Charity. 2013. GHDB. Luettu 3.9.2013. http://hackersforcharity.org/ghdb/

Hackers For Charity. 2004. Google Search: intitle:"Remote Desktop Web Connection". Luettu 8.11.2013
http://hackersforcharity.org/ghdb/?function=detail&id=118

Hackit. 2013. epdump. Luettu 10.11.2013.
http://hackit.org.ua/0201719568_snode146.html

IACRB. 2009. Certified Penetration Tester (CPT.) Luettu 7.7.2013.
http://www.iacertification.org/cpt_certified_penetration_tester.html

IACRB. 2009. Certified Expert Penetration Tester (CEPT.) Luettu 7.7.2013.
http://www.iacertification.org/cept_certified_expert_penetration_tester.html

IACRB. 2009. About IACRB. Luettu 7.7.2013.
http://www.iacertification.org/about-iacrb.htm

IANA.2013. Introducing IANA. Luettu 9.11.2013.
http://www.iana.org/about

IANA. 2013. Number Resources. Luettu 9.11.2013.
http://www.iana.org/numbers

ICANN. 2013. Welcome to ICANN!. Luettu 9.11.2013
http://www.icann.org/en/about/welcome

International Journal of Advanced Science and Technology. 2009. Penetration Testing for Hire. Luettu 6.11.2013
http://www.sersc.org/journals/IJAST/vol8/1.pdf

Internet Security Systems. 2013. SYN Flood. Luettu 15.11.2013.
http://www.iss.net/security_center/advice/Exploits/TCP/SYN_flood/default.htm

Internet Systems Consortium. 2013. BIND Software Status. Luettu 9.7.2013.
https://www.isc.org/downloads/software-support-policy/bind-software-status/

Internet Systems Consortium. 2013. The most widely used name server software: BIND. Luettu 9.7.2013.
http://www.isc.org/downloads/bind/

Internet Systems Consortium. 2013. BIND 9 Security Vulnerability Matrix. Luettu 9.7.2013.
https://kb.isc.org/article/AA-00913

Kennedy, D., O'Gorman, J., Kearns, D., Aharoni, M. 2011. Metasploit – The penetration tester's guide. No Starch Press. San Francisco.

Joe Keohan. 2010. Using Netcat To Spawn A Remote Shell. Luettu 13.11.2013.
http://jkeohan.wordpress.com/2010/04/30/using-netcat-to-spawn-a-remote-shell/

Klevinsky, T.J., Laliberte, S. & Gupta, A. 2002. Hack I.T. – Security Through Peneration Testing. Boston Pearson Education, Inc.

Know The Trade. 2013. Ethical Hacking – Footprinting. Luettu 8.11.2013
http://www.knowthetrade.com/footprinting.html

KPMG. 2013. Tietoturva. Luettu 7.7.13.
https://events.kpmg.fi/tietoturva.aspx

KPMG. 2013. CPTE. Luettu 6.11.2013.
https://events.kpmg.fi/Default.aspx?tabid=920&id=37743

KPMG. 2013. CPTC. Luettu 6.11.2013
https://events.kpmg.fi/Default.aspx?tabid=920&id=37744

LCPSoft. 2013. Screenshots. Luettu 3.12.2013.
http://www.lcpsoft.com/english/lcp/screenshots.html

lib.qrz.ru. 2013. Luettu 11.11.2013.
http://lib.qrz.ru/book/export/html/14451

Scott Lowe. 2008. A closer look at Windows Server 2008's Active Directory Users and Computers. Luettu 4.11.2013
http://www.techrepublic.com/blog/the-enterprise-cloud/a-closer-look-at-windows-server-2008s-active-directory-users-and-computers/364/

Michael J. Martin. 2002. Router Expert: Smurf/fraggle attack defense using SACLs. Luettu 15.11.2013.
http://searchnetworking.techtarget.com/tip/Router-Expert-Smurf-fraggle-attack-defense-using-SACLs

McAfee. 2013. Fpipe v2.1. Luettu 14.11.2013.
http://www.mcafee.com/us/downloads/free-tools/fpipe.aspx

McClure, S., Scambray, J., Kurtz, G. 2012. Hacking Exposed 7. McGraw-Hill Companies.

Microsoft. 2013. Port Assignments for Commonly-Used Services. Luettu 11.7.2013.
http://technet.microsoft.com/en-us/library/cc959833.aspx

Microsoft. 2013. Managing DHCP Scopes. Luettu 11.7.2013.
http://technet.microsoft.com/en-us/library/cc722532.aspx

Microsoft. 2013. Common Internet File System. Luettu 11.7.2013.
http://technet.microsoft.com/en-us/library/cc939973.aspx

Microsoft. 2013. Restrict Anonymous Check. Luettu 7.8.2013.
http://technet.microsoft.com/en-us/library/bb418944.aspx

Microsoft. 2013. Domain Secure Channel Utility -- Nltest.exe. Luettu 25.10.2013.
http://support.microsoft.com/kb/228477

Microsoft. 2013. Well-known security identifiers in Windows operating systems. Luettu 27.10.2013.
http://support.microsoft.com/kb/243330

Microsoft. 2013. Windows Interactive Logon Architecture. Luettu 4.11.2013
http://technet.microsoft.com/en-us/library/ff404303(v=ws.10).aspx

Microsoft 2013. The Structure of a DNS SOA Record. Luettu 9.11.2013.
http://support.microsoft.com/kb/163971

Microsoft. 2013. Internet Control Message Protocol (ICMP) Basics. Luettu 10.11.2013.
http://support.microsoft.com/kb/170292

Microsoft. 2013. Ask the Directory Service Team. Luettu 10.11.2013.
http://blogs.technet.com/b/askds/archive/2011/10/28/friday-mail-sack-they-pull-me-back-in-edition.aspx

Microsoft. 2008. Getting a CMD prompt as SYSTEM in Windows Vista and Windows Server 2008. Luettu 13.11.2013.
http://blogs.technet.com/b/askds/archive/2008/10/22/getting-a-cmd-prompt-as-system-in-windows-vista-and-windows-server-2008.aspx

mile2. 2013. Certified Penetration Testing Engineer. Luettu 7.7.2013.
http://mile2.com/penetration-testing-ethical-hacking/cpte.html

mile2. 2013. About Us. Luettu 7.7.13.
http://mile2.com/about-us.html

Mark Minasi. 1998. NLTEST. Luettu 25.10.2013.
http://windowsitpro.com/windows-server/nltest

Paul Mockapetris. 1987. DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION. Luettu 9.7.2013. http://tools.ietf.org/html/rfc1035

Paul Mockapetris. 1987. DOMAIN NAMES - CONCEPTS AND FACILITIES. Luettu 9.7.2013. http://tools.ietf.org/html/rfc1034

Willem Mouton. 2013. Finding Your Target. Luettu 9.11.2013
http://www.infosecisland.com/download/index/id/69.html

NIST. 2008. Technical Guide to Information Security Testing and Assessment. Luettu 5.11.2013
http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Nmap.org. 2013. Nmap Reference Guide. Luettu 15.11.2013.
http://nmap.org/book/man.html

NTA-wiki. 2009. Ike-scan User Guide. Luettu 28.10.2013.
http://www.nta-monitor.com/wiki/index.php/Ike-scan_User_Guide

Openwall. 2013. John The Ripper password cracker. Luettu 7.8.2013.
http://www.openwall.com/john/

Kevin Orrey. 2013. Pre-site Inspection. Luettu 5.11.2013
http://www.vulnerabilityassessment.co.uk/Presite%20Inspection.html

OWASP. 2009. Man-in-the-middle attack. Luettu 12.11.2013.
https://www.owasp.org/index.php/Man-in-the-middle_attack

Penetration Testing Lab. 2012. SMTP VRFY Sacnner. Luettu 10.11.2013.
http://pentestlab.wordpress.com/2012/11/26/smtp-vrfy-scanner/

Penetration Testing Lab. 2013. Dumpster Diving. Luettu 8.11.2013
http://pentestlab.wordpress.com/2013/03/28/dumpster-diving/

PTES. 2012. Pre-engagement. Luettu 12.6.2013.
http://www.pentest-standard.org/index.php/Pre-engagement

Brian Reed. 2011. Banner Grabbing (Ethical Hack). Luettu 10.11.2013.
http://www.firewalls.com/blog/banner_grab_ethical_hack/

Rebootuser. 2013. VulnVPN (Vulnerable VPN) Solutions. Luettu 11.11.2013.
http://www.rebootuser.com/?p=1474

RIPE Network Coordination Centre. 2013. Luettu 7.9.2013. https://www.ripe.net/

Michael Roth. 2006. Brute Force Hacking In Terminal Server Environments. Luettu 12.11.2013.
http://www.virtualizationadmin.com/articles-tutorials/terminal-services/security/brute-force-hacking-terminal-server-environments.html

Margaret Rouse. 2007. Smurfing. Luettu 15.11.2013.
http://searchsecurity.techtarget.com/definition/smurfing

Saarelainen, A. 2013. Kybersodan aseet. Tietokone 9/2013, 16-24.

Manish S. Saindane. 2013. Penetration Testing – A Systematic Approach. Luettu 15.7.2013.
http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf

Jason Samuel. 2012. How to fix pass-through authentication & the Windows 2008 logon screen on XenApp 6.5/Web Interface 5.4 using Citrix Receiver.Luettu 13.11.2013.
http://www.jasonsamuel.com/2012/01/05/how-to-fix-pass-through-authentication-the-windows-2008-logon-screen-on-xenapp-6-5web-interface-5-4-using-citrix-receiver/

The SANS Institute. 2013. Luettu 6.11.2013.
http://www.sans.org/

The SANS Institute. 2010. Identifying Loading Balancers in Penetration Testing. Luettu 6.11.2013.
http://www.sans.org/reading-room/whitepapers/testing/identifying-load-balancers-penetration-testing-33313

The SANS Institute. 2002. Penetration Testing – Is It Rigth For You. Luettu 2.12.2013.
https://www.sans.org/reading-room/whitepapers/testing/penetration-testing-you-265

The SANS Institute 2010. Writing a Penetration Testing Report. Luettu 12.11.2013.
http://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343

Sebastian Schreiber. 2009. Concept of a Professional Code of Ethics for Penetration Testers. Luettu 6.11.2013.
https://www.syss.de/fileadmin/ressources/040_veroeffentlichungen/dokumente/Code_of_Ethics_Penetration_Testers.pdf

Secunia ApS. 2013. Find out how many vulnerabilities were discovered in the 50 most popular programs in 2012. Luettu 12.11.2013
http://secunia.com/vulnerability-review/vulnerability_update_top50.html

James Shewmaker. 2006. Analyzing DLL Injection. Luettu 4.11.2013.
http://www.bluenotch.com/files/Shewmaker-DLL-Injection.pdf

The Sprawl. 2009. Host Discovery. Luettu 10.11.2013.
http://thesprawl.org/research/host-discovery/

Stanford University. 2007. Information Security Review Preliminary Questionnaire. Luettu 6.11.2013.
http://www.stanford.edu/group/security/securecomputing/SU_Security_Assess_v3.html

Eddie Sutton. 2013. Footprinting: What is it and How Do You Erase Them. Luettu 8.11.2013.
http://www.infosecwriters.com/text_resources/pdf/Footprinting.pdf

Tech Juice. 2011. Man-In-The-Middle Attacks with Ettercap. Luettu 15.11.2013.
http://www.tech-juice.org/2011/06/20/man-in-the-middle-attacks-with-ettercap/

The Measurement Factory. 2009. DNS SURVEY: OCTOBER 2009. Luettu 9.7.2013
http://dns.measurement-factory.com/surveys/200910.html

University Of South Wales. 2013. Windows Security – SMB – Server Message Blocks – Ports and Enumeration of Domain users and Trust relationships within the Domain. Luettu 10.11.2013.
http://uwnthesis.wordpress.com/2013/08/19/windows-security-smb-server-message-blocks/

Vesaria Network Security Specialists. 2013. Firewall Testing From Eye of the Hacker. Luettu 9.11.2013.
http://www.vesaria.com/Firewall/Testing/eye_of_hacker.php

Wai, C. 2002. Conducting a Penetration Test on an Organization. Luettu 13.6.2013.
http://www.sans.org/reading_room/whitepapers/auditing/conducting-penetration-test-organization_67

Web Applications Stack Exchange. 2012. How to modify a URL to get a Google cached version of page?. Luettu 8.11.2013.
http://webapps.stackexchange.com/questions/15633/how-to-modify-a-url-to-get-a-google-cached-version-of-page

Mike Williams. 2011. FOCA free 3.0. Luettu 8.11.2013.
http://www.downloadcrew.com/article/22211-foca_free

LIITTEET

Liite 1: DNSrecon tulokset

[*] Performing General Enumeration of Domain: wpk.tpu.fi
[-] DNSSEC is not configured for wpk.tpu.fi
[*] SOA palo3.wpk.tpu.fi 172.16.1.73
[*] NS palo3.wpk.tpu.fi 172.16.1.73
[*] NS palo2.wpk.tpu.fi 172.16.1.72
[*] NS palo4.wpk.tpu.fi 172.16.1.74
[*] MX pate.wpk.tpu.fi 172.16.1.56
[*] A wpk.tpu.fi 172.16.1.72
[*] A wpk.tpu.fi 172.16.1.73
[*] A wpk.tpu.fi 172.16.1.74
[*] A wpk.tpu.fi 172.16.1.90
[*] A wpk.tpu.fi 10.19.13.1
[*] Enumerating SRV Records
[*] SRV _gc._tcp.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74 3268 100
[*] SRV _kerberos._tcp.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74 88 100
[*] SRV _kerberos._tcp.wpk.tpu.fi palo3.wpk.tpu.fi 172.16.1.73 88 100
[*] SRV _kerberos._tcp.wpk.tpu.fi palo2.wpk.tpu.fi 172.16.1.72 88 100
[*] SRV _kerberos._udp.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74 88 100
[*] SRV _kerberos._udp.wpk.tpu.fi palo3.wpk.tpu.fi 172.16.1.73 88 100
[*] SRV _kerberos._udp.wpk.tpu.fi palo2.wpk.tpu.fi 172.16.1.72 88 100
[*] SRV _ldap._tcp.wpk.tpu.fi palo2.wpk.tpu.fi 172.16.1.72 389 100
[*] SRV _ldap._tcp.wpk.tpu.fi palo3.wpk.tpu.fi 172.16.1.73 389 100
[*] SRV _ldap._tcp.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74 389 100
[*] SRV _sipinternaltls._tcp.wpk.tpu.fi ocspool.wpk.tpu.fi 172.16.1.99 5061
[*] SRV _ldap._tcp.pdc._msdcs.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74 389
[*] SRV _ldap._tcp.gc._msdcs.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74 3268
[*] SRV_ldap._tcp.ForestDNSZones.wpk.tpu.fi palo2.wpk.tpu.fi 172.16.1.72
[*] SRV_ldap._tcp.ForestDNSZones.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74
[*] SRV_ldap._tcp.ForestDNSZones.wpk.tpu.fi palo3.wpk.tpu.fi 172.16.1.73
[*] SRV _ldap._tcp.dc._msdcs.wpk.tpu.fi palo2.wpk.tpu.fi 172.16.1.72 389
[*] SRV _ldap._tcp.dc._msdcs.wpk.tpu.fi palo3.wpk.tpu.fi 172.16.1.73 389
[*] SRV _ldap._tcp.dc._msdcs.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74 389
[*] SRV _kerberos._tcp.dc._msdcs.wpk.tpu.fi palo2.wpk.tpu.fi 172.16.1.72
[*] SRV _kerberos._tcp.dc._msdcs.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74
[*] SRV _kerberos._tcp.dc._msdcs.wpk.tpu.fi palo3.wpk.tpu.fi 172.16.1.73
[*] SRV _kpasswd._udp.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74 464 100
[*] SRV _kpasswd._udp.wpk.tpu.fi palo3.wpk.tpu.fi 172.16.1.73 464 100
[*] SRV _kpasswd._udp.wpk.tpu.fi palo2.wpk.tpu.fi 172.16.1.72 464 100
[*] SRV _kpasswd._tcp.wpk.tpu.fi palo4.wpk.tpu.fi 172.16.1.74 464 100
[*] SRV _kpasswd._tcp.wpk.tpu.fi palo3.wpk.tpu.fi 172.16.1.73 464 100
[*] SRV _kpasswd._tcp.wpk.tpu.fi palo2.wpk.tpu.fi 172.16.1.72 464 100

Liite 2: Fierce tulokset

```
root@bt:/pentest/enumeration/dns/fierce# ./fierce.pl -dns wpk.tpu.fi -wide
DNS Servers for wpk.tpu.fi:
        palo4.wpk.tpu.fi
        palo3.wpk.tpu.fi
        palo2.wpk.tpu.fi

Trying zone transfer first...
        Testing palo4.wpk.tpu.fi
                Request timed out or transfer not allowed.
        Testing palo3.wpk.tpu.fi
                Request timed out or transfer not allowed.
        Testing palo2.wpk.tpu.fi
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 1895 test(s)...
172.16.0.1      dhcp.wpk.tpu.fi
172.16.0.99     tuhkapilvi.wpk.tpu.fi
172.16.1.4      jauhe.wpk.tpu.fi
172.16.1.21     ahk.wpk.tpu.fi
172.16.1.30     arnold.wpk.tpu.fi
172.16.1.52     ulkodns.wpk.tpu.fi
172.16.1.54     luukku.wpk.tpu.fi
172.16.1.55     savu.wpk.tpu.fi
172.16.1.56     pate.wpk.tpu.fi
172.16.1.60     kellari.wpk.tpu.fi
172.16.1.62     hormi.wpk.tpu.fi
172.16.1.71     palo1.wpk.tpu.fi
172.16.1.72     palo2.wpk.tpu.fi
172.16.1.73     palo3.wpk.tpu.fi
172.16.1.74     palo4.wpk.tpu.fi
172.16.1.75     palo5.wpk.tpu.fi
172.16.1.76     palo6.wpk.tpu.fi
172.16.1.77     tankki.wpk.tpu.fi
172.16.1.78     tikas.wpk.tpu.fi
172.16.1.79     arina.wpk.tpu.fi
172.16.1.80     varoitin.wpk.tpu.fi
172.16.1.85     paloasema.wpk.tpu.fi
172.16.1.99     suutin.wpk.tpu.fi
172.16.1.28     master.wpk.tpu.fi
172.24.1.0      mc.wpk.tpu.fi
172.16.1.55     www.wpk.tpu.fi
Subnets found (may want to probe here using nmap or unicornscan):
        172.16.0.0-255 : 2 hostnames found.
        172.16.1.0-255 : 23 hostnames found.
        172.24.1.0-255 : 1 hostnames found.
```